



# M86 Enterprise Reporter

# USER GUIDE

## Administrator Console

Software Version: 6.0.10  
Document Version: 06.15.10

# M86 ENTERPRISE REPORTER ADMINISTRATOR USER GUIDE

© 2010 M86 Security  
All rights reserved.  
828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published June 2010 for software release 6.0.10

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from M86 Security.

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

The latest version of this document can be obtained from <http://www.m86security.com/support/Enterprise-Reporter/documentation.asp>

## **Trademarks**

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# ERS-UG\_v1.01-1006

---

# CONTENTS

<b>ENTERPRISE REPORTER OVERVIEW .....</b>	<b>1</b>
<b>Operations .....</b>	<b>1</b>
<b>How to Use this User Guide .....</b>	<b>2</b>
Organization .....	2
Conventions .....	3
Terminology .....	4
<b>ADMINISTRATOR SECTION .....</b>	<b>7</b>
<b>Introduction .....</b>	<b>7</b>
<b>Components and Environment .....</b>	<b>8</b>
Components .....	8
Hardware .....	8
Software .....	8
Environment .....	9
Workstation Requirements .....	9
Network Requirements .....	9
<b>Chapter 1: Accessing the Server .....</b>	<b>10</b>
Preliminary Network Settings .....	10
Procedures for Logging On, Off .....	10
Access the ER Administrator Login window .....	10
Log On .....	11
Logging on the First Time .....	13
Set up an Administrator Login ID .....	13
Log Off .....	14
<b>Chapter 2: Configuring the ER Server .....</b>	<b>15</b>
Administrator Console .....	15
Network Menu .....	15
Box Mode screen .....	16
Live Mode .....	16
Archive Mode .....	17
Change the Box Mode .....	17
Add/Edit/Delete Administrators screen .....	18

View a List of Administrators .....	19
Add an Administrator .....	19
Edit an Administrator's Login ID .....	19
Delete an Administrator .....	20
Locked-out Accounts and IPs screen .....	21
View Locked Accounts, IP addresses.....	22
Unlock Accounts, IP addresses .....	22
Network Settings screen .....	23
Set up/Edit IP Addresses.....	24
Routing Table screen .....	25
View a List of Routers.....	25
Add a Router.....	26
Delete a Router.....	26
Regional Setting screen .....	27
Specify the Time Zone.....	28
Specify the Language Set.....	28
Specify Network Time Protocol Servers .....	28
Update the Time on the Server.....	29
Network Diagnostics screen .....	30
Ping.....	31
Trace Route .....	32
SNMP screen .....	34
Enable SNMP .....	35
Set up Community Token for Public Access.....	35
Create, Build the Access Control List .....	35
Maintain the Access Control List .....	35
SSL Certificate screen .....	36
Generate an SSL Certificate for the ER.....	36
Server Menu .....	37
Backup screen .....	38
Backup and Recovery Procedures .....	38
Set up/Edit External Backup FTP Password .....	40
Execute a Manual Backup .....	40
Perform a Remote Backup .....	41
Perform a Restoration to the ER Server .....	42
Self Monitoring screen .....	43
View a List of Contact E-Mail Addresses.....	44
Set up and Activate Self-Monitoring .....	44
Remove Recipient from E-mail Notification List.....	44
Deactivate Self-Monitoring.....	44
SMTP Server Setting screen .....	45

Enter, Edit SMTP Server Settings .....	45
Verify SMTP Settings.....	46
Server Status screen.....	47
View the Status of the Server .....	48
Secure Access screen .....	49
Activate a Port to Access the Server .....	50
Terminate a Port Connection.....	51
Terminate All Port Connections .....	51
Software Update screen .....	52
View Installed Software Updates.....	53
Uninstall the Most Recently Applied Software Update .....	53
View Available Software Updates.....	53
Install a Software Update.....	54
Software Update Setting screen .....	57
Specify Proxy Settings.....	58
Save Settings.....	58
Shut Down screen .....	59
Server Action Selections.....	59
Perform a Server Action .....	60
Web Client Server Management screen .....	61
Restart the Web Client Server.....	61
Enable/Disable the Web Client Scheduler.....	62
Hardware Failure Detection screen .....	63
View the Status of the Hard Drives.....	63
Consolidated ER: Consolidated Mode Setting screen .....	65
View Remote ER Settings .....	65
Add a Remote ER.....	66
View Current Statistics for a Remote ER.....	66
Edit Settings for a Remote ER.....	67
Remove a Remote ER from the Consolidated ER.....	67
Database Menu .....	68
User Name Identification screen .....	68
View the User Name Identification screen.....	71
Configure the Server to Log User Activity.....	71
Deactivate User Name Identification .....	72
Username Display Setting screen .....	73
View the Current Username Display Setting .....	74
Modify the Username Display Setting.....	74
Page View Elapsed Time screen .....	76
Establish the Unit of Elapsed Time for Page Views.....	76
Elapsed Time Rules.....	77

- Page Definition screen ..... 78
  - View the Current Page Types ..... 78
  - Remove a Page Type ..... 79
  - Add a Page Type ..... 79
- Tools screen ..... 80
  - View Diagnostic Reports ..... 81
  - View Database Status Logs ..... 81
- Expiration screen ..... 84
  - Expiration Screen Terminology ..... 85
  - Expiration Rules ..... 86
  - View Data Storage Statistics ..... 87
  - Change Data Storage Settings ..... 90
- Optional Features screen ..... 92
  - Enable Search String Reporting ..... 94
  - Enable Block Request Count ..... 94
  - Enable Blocked Searched Keywords ..... 94
  - Enable Wall Clock Time ..... 95
  - Enable Page and/or Object Count ..... 95
  - Enable, Configure Password Security Option ..... 96
- User Group Import screen ..... 99
  - Import User Groups ..... 100

**TECHNICAL SUPPORT / PRODUCT WARRANTIES ..... 101**

- Technical Support ..... 101**
  - Hours ..... 101
  - Contact Information ..... 101
    - Domestic (United States) ..... 101
    - International ..... 101
  - E-Mail ..... 101
  - Office Locations and Phone Numbers ..... 102
    - M86 Corporate Headquarters (USA) ..... 102
    - M86 Taiwan ..... 102
  - Support Procedures ..... 103
- Product Warranties ..... 104**
  - Standard Warranty ..... 104
  - Technical Support and Service ..... 105
  - Extended Warranty (optional) ..... 106
  - Extended Technical Support and Service ..... 106

---

<b>APPENDICES SECTION .....</b>	<b>107</b>
<b>Appendix A .....</b>	<b>107</b>
Evaluation Mode .....	107
Administrator Console .....	107
Use the Server in the Evaluation Mode .....	109
Expiration screen .....	109
Change the Evaluation Mode .....	110
Activation Page .....	111
<b>Appendix B .....</b>	<b>112</b>
Disable Pop-up Blocking Software .....	112
Yahoo! Toolbar Pop-up Blocker .....	112
Add the Client to the White List .....	112
Google Toolbar Pop-up Blocker .....	114
Add the Client to the White List .....	114
AdwareSafe Pop-up Blocker .....	115
Disable Pop-up Blocking .....	115
Windows XP SP2 Pop-up Blocker .....	116
Set up Pop-up Blocking .....	116
Use the Internet Options dialog box .....	116
Use the IE Toolbar .....	117
Add the Client to the White List .....	118
Use the IE Toolbar .....	118
Use the Information Bar .....	119
Set up the Information Bar .....	119
Access the Client .....	119
<b>Appendix C .....</b>	<b>121</b>
RAID Maintenance and Troubleshooting .....	121
Part 1: Hardware Components .....	121
Part 2: Server Interface .....	122
LED indicators in SL and HL units .....	122
Front control panels on H, SL, and HL units .....	124
Rear panels on H and HL units .....	126
Part 3: Troubleshooting .....	127
Hard drive failure .....	127
Step 1: Review the notification email .....	127
Step 2: Verify the failed drive in the Admin console ...	128
Step 3: Replace the failed hard drive .....	129
Step 4: Rebuild the hard drive .....	130

- Step 5: Contact Technical Support..... 130
- Power supply failure..... 130
  - Step 1: Identify the failed power supply ..... 130
  - Step 2: Unplug the power cord ..... 130
  - Step 3: Replace the failed power supply ..... 131
  - Step 4: Contact Technical Support..... 131
- Fan failure ..... 132
  - Identify a fan failure ..... 132
- INDEX ..... 133**



# ENTERPRISE REPORTER OVERVIEW

Though many companies have Internet filtering solutions to prevent employees from accessing inappropriate, non-work related Web sites, simply blocking these sites is not enough. Administrators want the ability to know who is accessing which site, the duration of each site visit, and the frequency of these visits. This data can help administrators identify abusers, develop policies, and target sites to be filtered, in order to maximize bandwidth utilization and productivity.

The Enterprise Reporter (ER) from M86 Security is designed to readily obtain this information, giving the user the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained. This “view” can then be memorized and saved to a user-defined report menu for repetitive, scheduled execution and distribution.

## Operations

In simplified terms, the ER operates as follows: the ER Server module accepts log files (text files containing Web access data) from a source device such as the M86 Web Filter. M86 Security’s proprietary programs “normalize” the transferred data and insert them into a MySQL database. The ER Web Client reporting application accesses this database to generate a virtually unlimited number of queries and reports.

# How to Use this User Guide

## *Organization*

This User Guide is organized into the following sections:

- **Overview** - This section provides information on how to use this user guide to help you configure the ER Server.
- **Administrator Section** - Refer to this section for information on configuring and maintaining the ER Server via the Administrator console application.
- **Tech Support / Product Warranties Section** - This section contains information on technical support and product warranties.
- **Appendices Section** - Appendix A provides information on how to use the ER Server in the evaluation mode, and how to switch to the activated mode. Appendix B explains how to disable many types of pop-up blocking software. Appendix C includes information about RAID maintenance and troubleshooting on an ER “H”, “SL”, or “HL” server.
- **Index** - This section includes an index of topics and the first page numbers where they appear in this user guide.

## Conventions

The following icons are used throughout this user guide:



**NOTE:** *The “note” icon is followed by italicized text providing additional information about the current topic.*



**TIP:** *The “tip” icon is followed by italicized text giving you hints on how to execute a task more efficiently.*



**WARNING:** *The “warning” icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.*

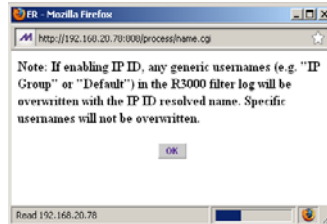


**IMPORTANT:** *The “important” icon is followed by italicized text informing you about important information or procedures to follow to ensure maximum uptime on the ER Server.*

## Terminology

The following terms are used throughout this user guide. Sample images (not to scale) are included for each item.

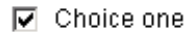
- **alert box** - a message box that opens in response to an entry you made in a dialog box, window, or screen. This box often contains a button (usually labeled “OK”) for you to click in order to confirm or execute a command.



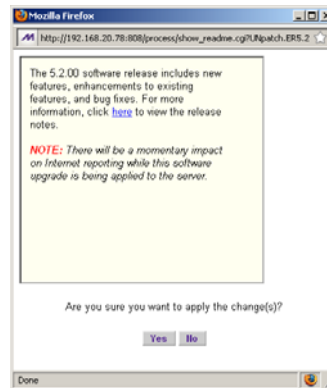
- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.



- **checkbox** - a small square in a dialog box, window, or screen used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an “X” is placed, indicating that you selected the option. When this box is not checked, the option is not selected.



- **dialog box** - a box that opens in response to a command made in a window or screen, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries or selections prior to clicking a button.



- **field** - an area in a dialog box, window, or screen that either accommodates your data entry, or displays pertinent information. A text box is a type of field.



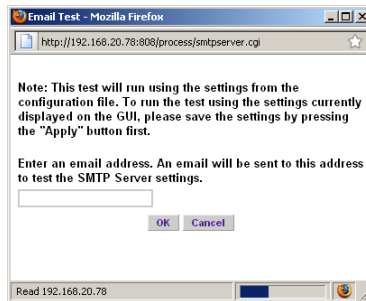
- **frame** - a boxed-in area in a dialog box, window, or screen that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function or purpose.



- **list box** - an area in a dialog box, window, or screen that accommodates and/or displays entries of items that can be added or removed.



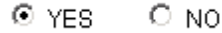
- **pop-up box or pop-up window** - a box or window that opens after you click a button in a dialog box, window, or screen. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.



- **pull-down menu** - a field in a dialog box, window, or screen that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.



- **radio button** - a small, circular object in a dialog box, window, or screen used for selecting an option. This object allows you to toggle between two choices. By clicking a radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option is not selected.



- **screen** - a main object of an application that displays across your monitor. A screen can contain windows, frames, fields, tables, text boxes, list boxes, buttons, and radio buttons.



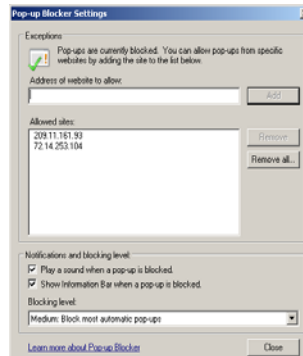
- **table** - an area in a window or screen that contains items previously entered or selected.

Destination	Gateway	Delete
1.1.1.1/1	1.1.1.1	<input type="checkbox"/>
1.2.3.4/1	1.3.2.4	<input type="checkbox"/>

- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field.



- **window** - displays on a screen, and can contain frames, fields, text boxes, list boxes, buttons, and radio buttons. Types of windows include ones from the system such as the Save As window, pop-up windows, or login windows.



# ADMINISTRATOR SECTION

## Introduction

The authorized administrator of the ER Server is responsible for integrating the Server into the existing network, and providing the Server a high speed connection to the designated logging device(s) and remote Client workstations. To attain this objective, the administrator performs the following tasks:

- executes Installation procedures defined in the ER Installation Guide booklet packaged with the ER Server
- provides a suitable environment for the Server, including:
  - high speed, HTTPS link to the current logging device
  - power connection protected by an Uninterruptible Power Supply (UPS)
  - high speed access to the Server by authorized Client workstations
- adds new administrators
- sets up administrators for receiving automatic alerts
- updates the Server with software updates supplied by M86 Security
- analyzes Server statistics
- utilizes diagnostics for monitoring the Server status to ensure optimum functioning of the Server
- establishes and implements backup and restoration procedures for the Server

Instructions on configuring and maintaining the ER Server are documented in this section.



**NOTE:** Click the **Help** link beneath the banner in any screen of the Administrator console to access a page with links to .pdf files of the latest user guides for the ER Administrator console and ER Web Client.

# Components and Environment

## Components

### Hardware

---

- High performance server
- One or more high-capacity hard drives
- Optional: One or more attached “NAS” storage devices (e.g. Ethernet connected, SCSI/Fibre Channel connected “SAN”)

### Software

---

- Linux OS
- Administrator Graphical User Interface (GUI) console utilized by an authorized administrator to configure and maintain the ER Server
- MySQL database
- M86 proprietary Client application employed by report users for generating “views” and reports



# Environment

## Workstation Requirements

---

System requirements for the administrator include the following:

- Windows XP, Vista, or 7 operating system running:
  - Internet Explorer (IE) 7.0 or 8.0
  - Firefox 3.5
- Macintosh OS X Version 10.5 or 10.6 running:
  - Safari 4.0
  - Firefox 3.5
- Pop-up blocking software, if installed, must be disabled
- Session cookies from the ER Server must be allowed in order for the Administrator console to function properly



**NOTE:** Information about disabling pop-up blocking software can be found in Appendix B: Disable Pop-up Blocking Software.

## Network Requirements

---

- High speed connection from the ER Server to the Web access logging device(s)
- High speed connection from the ER Server to the Client workstation(s)
- HTTPS connection to M86 Security's software update server

# Chapter 1: Accessing the Server

## *Preliminary Network Settings*

To initially set up your ER Server, follow the instructions in the ER Installation Guide booklet packaged with your ER unit. This guide explains how to perform the initial configuration of the Server so that it can be accessed via an IP address on your network.



**NOTE:** *If you do not have the ER Administrator Installation Guide, contact M86 Security immediately to have a copy sent to you.*



**WARNING:** *In order to prevent data from being lost or corrupted while the Server is running, the Server should be connected to a UPS or other battery backup system.*

## *Procedures for Logging On, Off*

### Access the ER Administrator Login window



**WARNING:** *Once you turn on the Server, **DO NOT** interrupt the initial boot-up process. This process may take from five to 10 minutes per drive. If the process is interrupted, damage to key files may occur.*

When the Server is fully booted, any workstation on the network that can access the Server's IP address (set up during installation procedures) will be able to communicate with the Server via the Internet.

1. Launch an Internet browser window supported by the ER Server.
2. In the address line of the browser window, type in "https://", and the ER Server's IP address or host name, and use port number ":8843" for a secure network connection.

For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:8843**. Using a host name example, if the host name is logo.com, type in **https://logo.com:8843**.

With a secure connection, the first time you attempt to access the ER Server's user interface in your browser you will be prompted to accept the security certificate. In order to accept the security certificate, follow the instructions at: <http://www.m86security.com/software/8e6/docs/ig/misc/sec-cert-er.pdf>

3. After accepting the security certificate, click **Go** to open the ER Administrator Login window (see Fig. 1:1-1).

## Log On

1. In the login window, type in the generic Username **admin**, and Password **reporter**, if you have not yet set up your own user name and password. Otherwise, enter your personal **Username** and **Password**:



Fig. 1:1-1 Login window

2. Click **Login** to go to the default Server Status screen of the Administrator console (see Fig. 1:1-2).



**NOTES:** If using a consolidated ER server, some screens in the Administrator console differ; there are a few unique screens, and some screens are not included. The Consolidated Mode icon (shown at right) displays to the right in the navigation bar on each screen.



A consolidated ER Server (CER) is used in environments with multiple ER Servers, and acts as the source for consolidating records from all remote ER Servers added in the Administrator console. See the ER Web Client User Guide for information on using the Web Client with a CER Server.

**Enterprise Reporter**

Network Server Database [Help](#) [Logout](#)

**Product Version:**  
Enterprise Reporter  
Version 6.0.10.1  
March 11, 2010  
Copyright 2010 M86 Security

**Server Status**

**CPU Utilization**

**CPU Load Averages:** 1.38, 1.59, 1.32  
**CPU states:** 0.9%us, 0.5%sy, 0.0%ni, 96.8%id, 1.8%wa, 0.0%hi, 0.0%si, 0.0%st  
**Memory:** 4151508k total, 3911804k used, 239704k free, 38204k buffers  
**Swap:** 2097144k total, 84k used, 2097060k free, 2335500k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3507	dbus	20	0	2712	860	700	S	0	0.0	0:00.00	dbus-daemon
30011	root	20	0	7024	1964	1404	S	0	0.0	0:43.48	dbcontrol

**Disk drives status**

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
29931580	1730224	26680924	7%	/	
none	2075752	0	2075752	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
79473544	2477232	72959296	4%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
128951204	7862204	112640260	7%	/backup	
/dev/mapper/VG00-dblv1					
219112724	186212228	32900496	85%	/database/d1	

**NETSTAT**

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	enii-md.qc.8e6.net:mysql	192.168.30.92:ums	ESTABLISHED	3667/mysqlqd
tcp	0	0	ERSL.121.8e6.com:mysql	ERSL.121.8e6.com:40985	ESTABLISHED	3667/mysqlqd
tcp	0	0	enii-md.qc.8e6.net:mysql	192.168.30.92:nstp	ESTABLISHED	3667/mysqlqd

Fig. 1:1-2 Server Status screen

The Server Status screen displays the current status of the ER Server.



**NOTES:** See Server Status screen in the Server section of this document for information about the contents and usage of this screen.

If using this product in the Evaluation Mode the ER Status pop-up window opens after logging into this application. Please see Appendix A: Evaluation Mode for information about the Evaluation Mode.

## Logging on the First Time

### Set up an Administrator Login ID



**NOTE:** If you have already set up your user name and password, you can skip this section.

1. At the Network pull-down menu, choose **Administrators** to display the Add/Edit/Delete Administrators screen where you set up your user name and password:

The screenshot shows the 'Enterprise Reporter' application interface. At the top, there is a navigation bar with 'Enterprise Reporter' and the 'M86 SECURITY' logo. Below this is a menu bar with 'Network', 'Server', and 'Database' dropdown menus, and 'Help Logout' links. The main content area displays a modal window titled 'Add/Edit/Delete Administrators'. Inside this window, there is a dropdown menu labeled 'New Administrator' with a downward arrow. Below it are three input fields: 'User Name' containing the text 'admin', 'Password' with masked characters (dots), and 'Confirm Password' which is empty. At the bottom of the modal window are two buttons: 'Save' and 'Delete'.

Fig. 1:1-3 Add/Edit/Delete Administrators screen

2. Select **New Administrators** from the pull-down menu.

3. In the **User Name** field, enter up to 20 characters—this may include upper- and/or lowercase alphanumeric characters, and special characters.
4. In the **Password** field, enter eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
5. In the **Confirm Password** field, re-enter the password in the exact format used at the Password field.
6. Click the **Save** button.

## Log Off

---

To log off the Administrator console, click the **Logout** link beneath the banner in any screen to display the logout window:

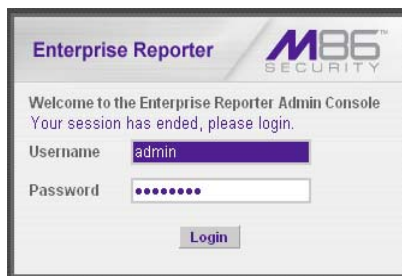


Fig. 1:1-4 Logout window

Click the “X” in the upper right corner of the browser window/tab to close the logout window. Exiting the Administrator console will log you off the Server, but will not turn off the Server.



**WARNING:** If you need to turn off the Server, follow the shut down procedures outlined in the Shut Down screen sub-section under the Server Menu section in Chapter 2. Failure to properly shut down the Server can result in data being lost or corrupted.

# Chapter 2: Configuring the ER Server

## ***Administrator Console***

The Administrator console is used for configuring and maintaining the ER Server. Settings made in the Administrator console affect the Client reporting application. The Administrator console includes three menus: Network, Server, and Database. Each menu contains options from which you make selections to access screens used for configuring your Server.



**TIP:** *When making a complete configuration of the Server, M86 Security recommends you navigate from left to right (Network to Server to Database) in choosing your menu options.*

## **Network Menu**

---

The Network pull-down menu includes options for setting up and maintaining components to be used on the Server's network. These options are: Box Mode, Administrators, Lockouts, Network Setting, Routing Table, Regional Setting, Diagnostics, SNMP, and SSL Certificate.

## Box Mode screen

The Box Mode screen displays when the Box Mode option is selected from the Network menu. The box mode indicates whether the Server box is functioning in the “live” mode, or in the “archive” mode. When the box mode displays on the screen, you can view the current mode set for the Server, and can change this setting, if necessary.



Fig. 1:2-1 Box Mode screen

### Live Mode

Once your Server is configured and the Server box is set in the “live” mode, it will receive and process real time data from the Web access logging device. The Client reporting application can then be used to capture data and create views.



## Archive Mode

In the “archive” mode, the Server box solely functions as a receptacle in which historical, archived files are placed. In this mode, “old” files placed on the Server can be viewed using the Client reporting application.

## Change the Box Mode

1. Click the **Change Mode** button to display the two box mode options on the screen:



Fig. 1:2-2 Change Box Mode

2. Click the radio button corresponding to **Live** or **Archive** to specify the mode in which the Server should function:
  - choose **Live** if you wish the Server to function in the “live” mode, receiving and processing real time data from the Web access logging device.

- choose **Archive** if you wish the Server to function in the “archive” mode, solely as a receptacle for historical, archived files. In this mode, “old” files placed on the Server can be viewed using the Client reporting application.
3. Click **Apply** to confirm your selection. The mode you specify will immediately be in effect.



**NOTE:** After applying the box mode setting, you must restart the Server by selecting the **Restart Hardware** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)

## Add/Edit/Delete Administrators screen

The Add/Edit/Delete Administrators screen displays when the Administrators option is selected from the Network menu. This screen is used for viewing, adding, editing, and deleting the login ID of personnel authorized to configure the Server.

The screenshot shows the Enterprise Reporter web interface. At the top, there is a navigation bar with "Enterprise Reporter" and the "M86 SECURITY" logo. Below the navigation bar are three dropdown menus: "Network", "Server", and "Database". To the right of these menus are "Help" and "Logout" links. The main content area is titled "Add/Edit/Delete Administrators". Inside this area, there is a form with the following fields and controls:

- A dropdown menu labeled "New Administrator" with a downward arrow.
- A text input field labeled "User Name" containing the text "admin".
- A text input field labeled "Password" containing seven dots.
- A text input field labeled "Confirm Password" which is currently empty.
- Two buttons at the bottom: "Save" and "Delete".

Fig. 1:2-3 Add/Edit/Delete Administrators screen



**TIPS:** For security purposes, administrators should be the first users set up on the Server. M86 Security recommends adding an alternate login ID prior to editing or deleting the default login ID. By doing so, if one login ID fails, you have another you can use.

### ***View a List of Administrators***

To view a list of administrator user names, click the down arrow at the **New Administrator** field. If no administrator has yet been assigned to the Server, no selections display except for the default “admin” user name.

### ***Add an Administrator***

1. Select **New Administrator** from the pull-down menu.
2. In the **User Name** field, enter up to 20 characters—this may include upper- and/or lowercase alphanumeric characters, and special characters.
3. In the **Password** field, enter eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
4. In the **Confirm Password** field, re-enter the password in the exact format used in the Password field.
5. Click the **Save** button to add the administrator to the choices in the pull-down menu.

### ***Edit an Administrator’s Login ID***

1. Select the administrator’s user name from the pull-down menu.
2. Edit either of the following fields:
  - User Name
  - Password (if this field is edited, the Confirm Password field must be edited in tandem)

3. Click the **Save** button.

### ***Delete an Administrator***

1. Select the administrator's user name from the pull-down menu.
2. After the administrator's login ID information populates the fields, click the **Delete** button to remove the administrator's user name from the choices in the pull-down menu.

## Locked-out Accounts and IPs screen

The Locked-out Accounts and IPs screen displays when the Lockouts option is selected from the Network menu. This screen is used for unlocking accounts or IP addresses of administrators and sub-administrators that are currently locked out of the Administrator console or Web Client.

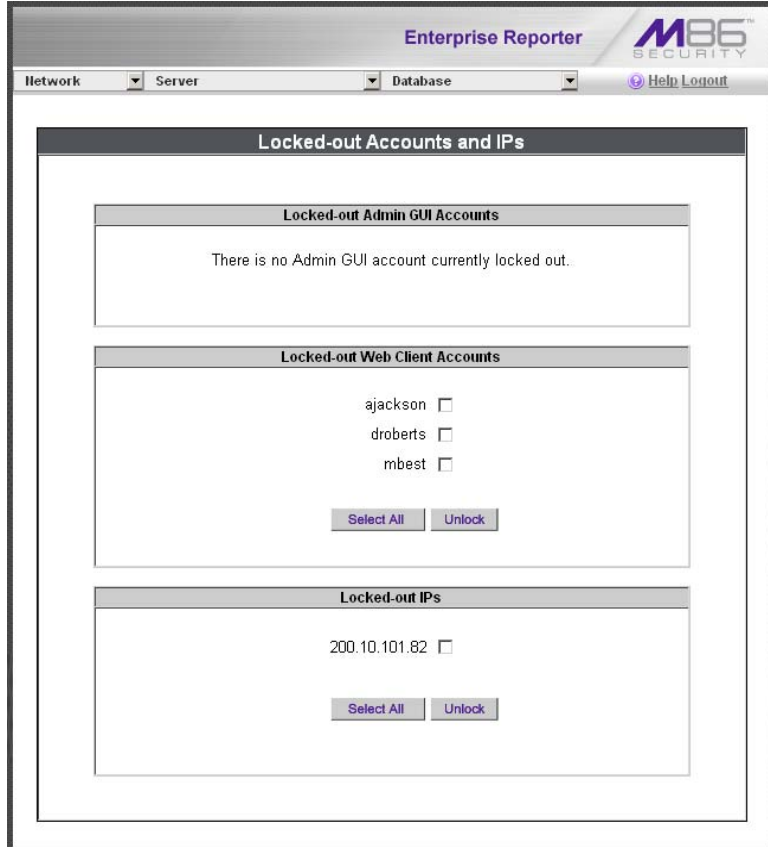


Fig. 1:2-4 Locked-out Accounts and IPs screen



**NOTE:** An account or IP address becomes locked if the Password Security Options feature is enabled in the Optional Features screen, and a user is unable to log into the Administrator console or Web Client due to a password expiration, or having met the specified number of failed password attempts within the designated timespan.

### **View Locked Accounts, IP addresses**

The frames in this screen display the following messages if there are no users currently locked out:

- **Locked-out Admin GUI Accounts** - There is no Admin GUI account currently locked out.
- **Locked-out Web Client Accounts** - There is no Web Client account currently locked out.
- **Locked-out IPs** - There is no IP currently locked out.

If there are any locked accounts/IP addresses in a frame, each locked username/IP address displays on a separate line followed by a checkbox. The Select All and Unlock buttons display at the bottom of the frame.

### **Unlock Accounts, IP addresses**

To unlock an account/IP address in a frame:

1. Click the checkbox corresponding to the username/IP address.



**TIP:** To unlock all accounts/IPs in a frame, click **Select All** to populate all checkboxes in the frame with check marks.

2. Click **Unlock** to unlock the specified accounts/IPs, and to display the message screen showing one of the following pertinent messages for each unlocked account/IP:
  - Admin account: 'xxx' has been successfully unlocked.
  - Web client account: 'xxx' has been successfully unlocked.

- IP: 'x.x.x.x' has been successfully unlocked.



**NOTE:** In the text above, 'xxx' and 'x.x.x.x' represents the unlocked username/IP address.

3. Click **OK** to return to the Locked-out Accounts and IPs screen that no longer shows the accounts/IPs that have been unlocked.

## Network Settings screen

The Network Settings screen displays when the Network Setting option is selected from the Network menu. This screen is used for setting up IP addresses so the Server can communicate with your system.

The screenshot shows the Enterprise Reporter interface. At the top, there is a navigation bar with 'Enterprise Reporter' and the M86 SECURITY logo. Below the navigation bar are dropdown menus for 'Network', 'Server', and 'Database', along with 'Help' and 'Logout' links. The main content area displays a 'Network Settings' dialog box. Inside this dialog, there is a 'Network' section with the following fields and values:

Network	
Host Name	SR64-20-78.qc.net
LAN 1 IP	192.168.20.78
Netmask	255.255.0.0
Gateway IP	192.168.20.1
First DNS IP	192.168.168.200
Second DNS IP	192.168.20.1

A 'Save' button is located at the bottom of the form.

Fig. 1:2-5 Network Settings screen

## Set up/Edit IP Addresses



**TIP:** In order for the Server to effectively communicate with your system, be sure all fields contain accurate information before saving your settings.

1. Enter or edit an IP address in each appropriate field:
  - In the **Host Name** field, enter the address or URL that will be used for accessing the Administrator console. This entry should include the full, qualified domain name, and the “host” name for the box (i.e. reporter.myserver.com).
  - In the **LAN 1 IP** field, enter the IP address of the ER Server on your Local Area Network (LAN 1).
  - In the **Netmask** field, enter the netmask that will define the traffic designated for the LAN.
  - In the **Gateway IP** field, enter the IP address for the default router that will be the main gateway for the entire network segment.
  - In the **First DNS IP** field, enter the IP address of the primary Domain Name System (name server). The Server box will use this IP address to identify other IP addresses on the system, including its own IP address.
  - In the **Second DNS IP** field, enter the IP address of the fallback DNS.
2. Be sure each IP address is correct, and then click **Save**.



**NOTE:** After appropriate entries have been made in these fields and saved, you must restart the Server to activate the IPs. To restart the Server, select the **Restart Hardware** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)



## Routing Table screen

The Routing Table screen displays when the Routing Table option is selected from the Network menu. This screen is used for viewing, building, and maintaining a list of routers—network destination and gateway IP addresses—the Server will use for communicating with other segments of the network. You will only need to set up a routing table if your local network is interconnected with another network.



Fig. 1:2-6 Routing Table screen

### View a List of Routers

Each router that was configured in the routing table displays as a separate row in the table. The IP address and subnet mask to receive data packets display in the Destination column, and the IP address of the portal that will transfer data packets to and from the Internet displays in the Gateway column.

### ***Add a Router***

1. In the **Destination** field, enter the IP address of the network to which data packets will be forwarded.
2. At the **Network Mask** pull-down menu, specify the number (1-32) of the subnet mask that will be used for grouping IP addresses on the same local network.
3. In the **Gateway** field, enter the IP address of the portal to which data packets will be transferred to and from the Internet.
4. Click the **Add** button to include your entry in the table. If you have another router to add, follow steps 1-4.
5. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

### ***Delete a Router***

1. Click in the **Delete** checkbox of the row corresponding to the router you wish to remove from the routing table.
2. Click the **Delete** button.
3. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

## Regional Setting screen

The Regional Setting screen displays when the Regional Setting option is selected from the Network menu. This screen is used for specifying the time zone and network time to be used by the Server when generating reports via the Client application, and setting the language set type to be displayed in the Administrator console, if necessary.

The screenshot shows the 'Regional Setting' screen within the 'Enterprise Reporter' application. The interface includes a navigation bar with 'Network', 'Server', and 'Database' menus, and a 'Help Logout' link. The main content area is divided into three sections:

- Time Zone:** Features 'Region' and 'Location' dropdown menus, a 'Save' button, and a warning: 'Warning: This will Reboot the Enterprise Reporter System.'
- Language:** Features a 'Language' dropdown menu, a 'Save' button, and a warning: 'Warning: Saving the language will restart the web client server.'
- NTP Server:** Includes a text input for 'Enter local network time protocol (NTP):' and three text inputs for 'Server 1', 'Server 2', and 'Server 3'. The current values are 128.59.35.142, 142.3.100.15, and 129.132.98.11. It also has 'Save' and 'NTP Update' buttons.

At the bottom of the screen, it displays 'Current ER server system time: Tue Dec 22 16:29:22 2009'.

Fig. 1:2-7 Regional Setting screen

## ***Specify the Time Zone***

1. At the **Region** pull-down menu, select your country from the available choices.
2. At the **Location** pull-down menu, select the time zone for the specified region.
3. Click **Save** to apply your settings, and to restart the Web Client Server.



**WARNING:** *The time zone set for the ER should be the same one set for each Web access logging device to be used by the ER. These “like” settings ensure consistency when tracking the logging times of all users on the network.*

## ***Specify the Language Set***

1. If necessary, select a language set from the **Language** pull-down menu to specify that you wish to display that text in the console.
2. Click **Save** to apply your settings, and to restart the Web Client Server.

## ***Specify Network Time Protocol Servers***

IP addresses of servers running Network Time Protocol (NTP) software are entered in the Server fields, and the Current ER server system time (day, date, HH:MM:SS time format, and year) displays below. NTP is a time synchronization system for computer clocks throughout the Internet. Your ER Server will use the actual time from clocks at the IP addresses you've specified.

For the Enter local network time protocol (NTP) server fields, by default, the following IP addresses display in these three fields: 128.59.35.142, 142.3.100.15, and 129.132.98.11. If you wish to use different NTP servers, follow these steps:

1. Enter or edit an IP address in each appropriate field:
  - In the **Server 1** field, enter the IP address of the primary NTP server to be used for clock settings on your Server.
  - In the **Server 2** field, enter the IP address of the secondary NTP server. The time from this server will be used by your Server if the IP address for the primary server fails to be accessed by your Server.
  - In the **Server 3** field, enter the IP address of the tertiary NTP server. The time from this server will be used by your Server if the IP addresses for the primary and secondary servers fail to be accessed by your Server.
2. Click the **Save** button to save your entries.



**NOTE:** *When you click the Save button, the IP addresses you entered are saved, but the time on your Server will not be synchronized with the NTP servers until you click the NTP Update button.*

### ***Update the Time on the Server***

After you have saved the IP addresses of NTP servers you wish your Server to access, click the **NTP Update** button to synchronize the clock on your Server with the NTP server clocks.

## Network Diagnostics screen

The Network Diagnostics screen displays when the Diagnostics option is selected from the Network menu. This screen is used to help you identify and resolve problems with your network configuration, using the ping and trace route utility tools.

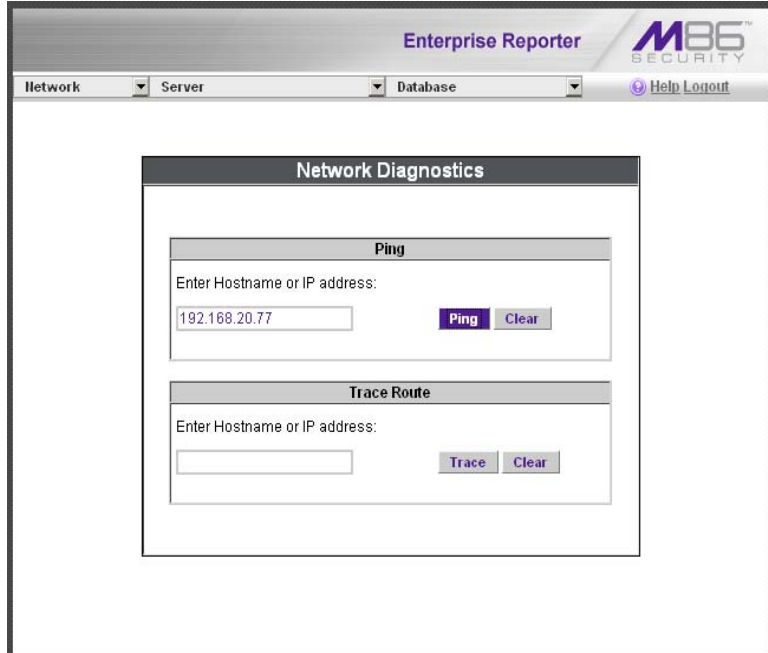


Fig. 1:2-8 Network Diagnostics screen, Ping entry

## Ping

The ping utility is used for verifying whether the Server can communicate with a machine at a given IP address within the network, and the speed of the network connection.

1. In the Ping frame, enter the IP address or host name of the specific Internet address to be contacted (pinged).
2. Click the **Ping** button to display the results found by the Server, as shown on the sample screen:

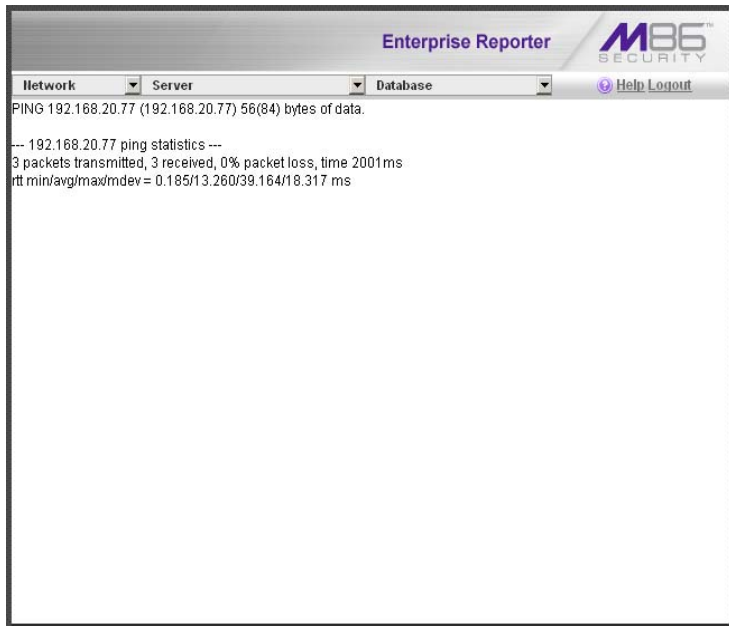


Fig. 1:2-9 Ping results

As indicated by the results for the sample entry, the Server at 192.168.20.78 was able to communicate with the machine at the IP address 192.168.20.77. The statistics show that three (3) data packets were transmitted by the Server, and three (3) packets were received by the designated machine, for a total of zero (0) percent packet loss.



**TIP:** If the machine cannot be contacted, be sure the ping feature on that machine is turned on.



**NOTE:** To ping another IP address, click the Back button in your browser window, then click the Clear button in the Ping frame, and follow the procedures documented in this sub-section.

## Trace Route

If the ping utility was not able to help you diagnose the problem with your network configuration, you should use the trace route utility. This diagnostic tool records each “hop” (trip from one router to another) the data packet made, identifying the IP addresses of gateway computers where the packet stopped en route to its final destination, and the length of time of each hop.



**NOTE:** The trace route utility can be used after your routing table has been set up. To set up a routing table, see the Routing Table screen sub-section under the Network menu in this chapter.

1. In the Trace Route frame, enter the IP address or host name of the specific Internet address to be validated.
2. Click the **Trace** button to display the results found by the Server, as shown on the sample screen:



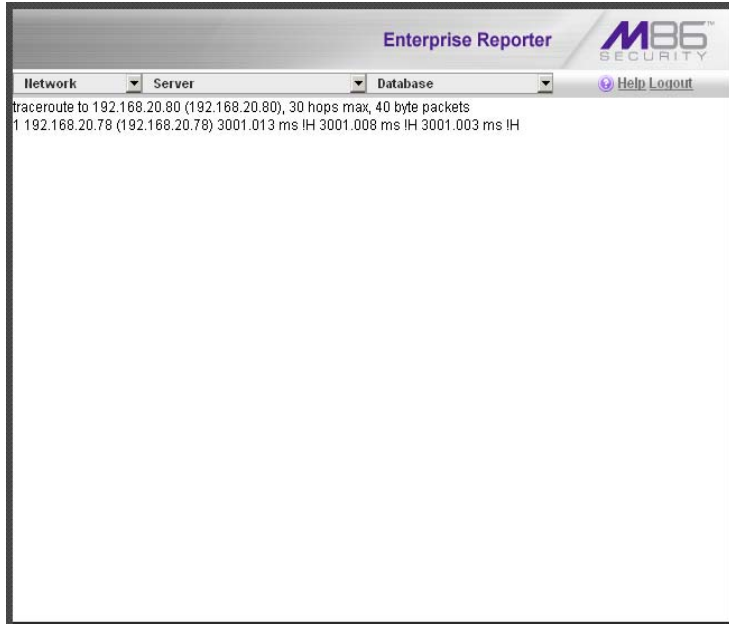



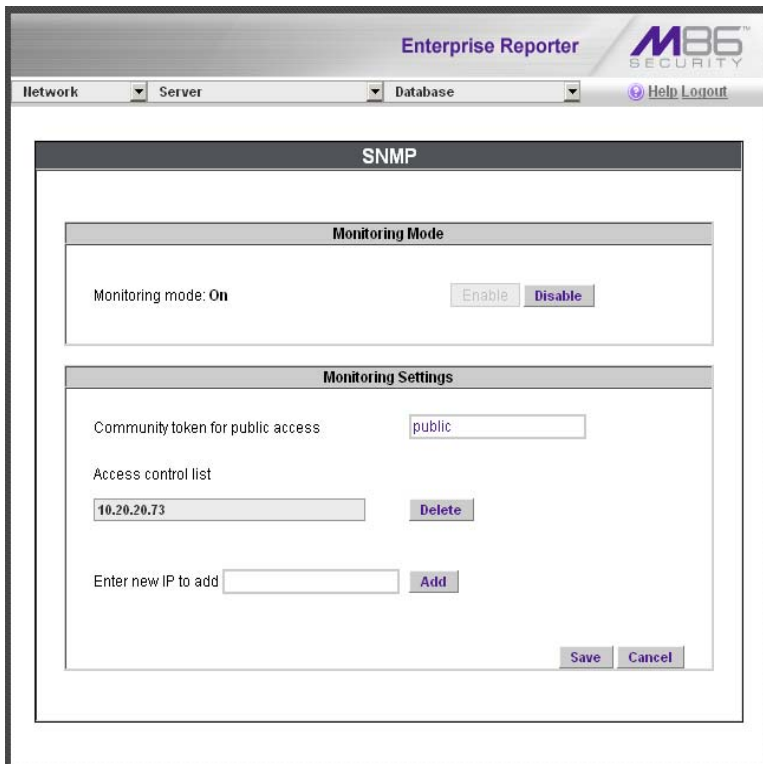
Fig. 1:2-10 Trace Route results

As indicated by the results for the sample entry, the packet made 30 hops. For each line in the report, the hop number displays, followed by the IP address or host name; the IP address in parentheses; and the maximum, minimum, and average response time in milliseconds.

 **TIP:** To “trace” another IP address, click the Back button in your browser window, then click the Clear button in the Trace Route frame, and follow the procedures documented in this subsection.

## SNMP screen

The SNMP screen displays when the SNMP option is selected from the Network menu. This feature lets the global administrator use a third party Simple Network Management Protocol (SNMP) product for monitoring and managing the working status of the ER's Internet reporting on a network.



The screenshot shows the 'Enterprise Reporter' web interface. At the top, there is a navigation bar with 'Enterprise Reporter' and the 'M86 SECURITY' logo. Below the logo are dropdown menus for 'Network', 'Server', and 'Database', and a 'Help Logout' link. The main content area is titled 'SNMP' and is divided into two sections: 'Monitoring Mode' and 'Monitoring Settings'. In the 'Monitoring Mode' section, 'Monitoring mode: On' is displayed, with 'Enable' and 'Disable' buttons. The 'Monitoring Settings' section includes a 'Community token for public access' field with the value 'public'. Below this is an 'Access control list' section with a table containing the IP address '10.20.20.73' and a 'Delete' button. At the bottom of this section, there is an 'Enter new IP to add' field and an 'Add' button. Finally, 'Save' and 'Cancel' buttons are located at the bottom right of the main content area.

Fig. 1:2-11 SNMP screen

The following aspects of the ER are monitored by SNMP: data traffic sent/received by a NIC, CPU load average at a given time interval, amount of free disk space for each disk partition, time elapse since the box was last rebooted, and the amount of memory currently in usage.

### ***Enable SNMP***

The **Monitoring mode** is “Off” by default. To enable SNMP, click **Enable** in the Monitoring Mode frame. As a result, all elements in this window become activated.

### ***Set up Community Token for Public Access***

Enter the password to be used as the **Community token for public access**. This is the password that the management console would use when requesting access.

### ***Create, Build the Access Control List***

1. In the **Enter new IP to add** field, enter the IP address of an interface from/to which the SNMP should receive/send data.
2. Click **Add** to include the entry in the Access control list box.

Repeat steps 1 and 2 for each IP address to be included in the list.

3. After all entries are made, click **Save**.

### ***Maintain the Access Control List***

1. To remove one or more IP addresses from the list, select each IP address from the Access control list, using the **Ctrl** key for multiple selections.
2. Click **Delete**.
3. Click **Save**.

## SSL Certificate screen

The SSL Certificate screen displays when the SSL Certificate option is selected from the Network menu. This screen is used for generating an SSL certificate for the ER Server to ensure a Secure Sockets Layer connection between the server and your browser.



Fig. 1:2-12 SSL Certificate screen

### Generate an SSL Certificate for the ER

1. Click **Generate SSL Certificate** to display the page that asks if you wish to continue, which would restart your server.



**TIP:** Click **No** to return to SSL Certificate screen.

2. Click **Yes** to generate the SSL certificate and restart the ER Server.

3. Close your browser and wait a few minutes before attempting to access the user interface.

## Server Menu

---

The Server pull-down menu includes options for setting up processes for maintaining the Server. These options are: Backup, Self-Monitoring, SMTP Server Setting, Server Status, Secure Access, Software Update, Software Update Setting, Shut Down, Web Client Server Management, and Hardware Failure Detection.



**NOTES:** *The Software Update Setting option is only available if the Web Filter unit is set up in the Stand Alone mode. See the Synchronization sub-section in the M86 Web Filter User Guide for more information about setup modes.*

*An additional option for Consolidated Mode Setting is available on a consolidated ER Server (CER). See Consolidated ER: Consolidated Mode Setting screen for details on how to configure this option.*

## Backup screen

The Backup screen displays when the Backup option is selected from the Server menu. This screen is used for setting up the password for the remote server's FTP account, for executing an immediate backup on the ER Server, and for performing a restoration to the database from the previous backup run.

The screenshot shows the 'Backup' screen in the Enterprise Reporter application. At the top, there is a navigation bar with the 'Enterprise Reporter' logo and 'M86 SECURITY' logo. Below the navigation bar are three dropdown menus: 'Network', 'Server', and 'Database'. The main content area is titled 'Backup' and contains two sections:

- External Backup FTP Account:** This section contains a text box stating 'This creates FTP login account to allow FTP access to ER.' Below this are three input fields: 'Username' (containing 'ERbackup'), 'Password' (masked with dots), and 'Confirm Password'. An 'Apply' button is located below the 'Confirm Password' field.
- Internal Backup Restore Action:** This section contains two warning messages and two buttons. The first warning says 'Warning: This will backup your live data to ER internal backup drive.' and has a 'Manual Backup' button below it. The second warning says 'Warning: This will override your current database with internal backup data.' and has a 'Manual Restore' button below it.

Fig. 1:2-13 Backup screen

## Backup and Recovery Procedures

**!** **IMPORTANT:** M86 Security recommends establishing backup and recovery procedures when you first begin using the ER Server. Please follow the advice in this section to ensure your ER Server is properly maintained in the event that data is lost and back up procedures need to be performed to recover data.

Although automatic backups to a local ER hard drive are scheduled nightly by default, it is important that the ER administrator implements a backup policy to ensure data integrity and continuity in the event of any possible failure scenario. This policy should include frequent, remote backups, such that raw logs and ER database files are available for restoration without relying on the ER's hard drives.

In general, recovery plans involve (i) restoring the most recent backup of the database, and (ii) restoring raw logs to fill in the gap between the most recent backup of the database, and the current date and time.

Some scenarios and action plans to consider include the following:

- **The ER database becomes corrupted** - Correct the root problem. Restore the database from the most recent ER backup, and reprocess raw logs up to the current date and time.
- **The data drive fails** - Replace the data drive. Restore the database from the ER backup drive, and reprocess raw logs up to the current date and time.
- **The backup drive fails** - Replace the backup drive, and perform a manual backup.
- **Both data and backup drives are damaged** - Restore the database from the most recent remote backup, and reprocess raw logs up to the current date and time.

As you can see, it is critical that raw logs are available to bridge the gap between the last database backup and the present time, and more frequent backups (local and remote) result in less “catch-up” time required for reprocessing raw logs.

## Set up/Edit External Backup FTP Password

In order to back up the ER Server's database to a remote server, an FTP account must be established for the remote server.



**NOTE:** In the External Backup FTP Account frame, the login name that will be used to access the remote server displays in the Username field. This field cannot be edited.

1. In the **Password** field, enter up to eight characters for the password. The entry in this field is alphanumeric and case sensitive.
2. In the **Confirm Password** field, re-enter the password in the exact format used in the Password field.
3. Click the **Apply** button to save your entries. The updated Account ID will be activated after two minutes.

## Execute a Manual Backup

In addition to performing on demand backups in preparation for a disaster recovery, you may wish to execute a manual backup under the following circumstances:

- **Power outage** - If there is a power outage at your facility and your system uses a backup battery, you might want to back up data before the battery fails.
- **Rolling blackout** - If your facility is subjected to rolling blackouts, and a blackout is scheduled during the time of your daily backup, you should back up your data before the blackout period, when the ER Server will be down.
- **Expiration about to occur** - If a data expiration is about to occur, you might want to back up your data before losing the oldest data on the ER Server, prior to the daily backup process.



**WARNING:** If corrupted data is detected on the ER Server, do not backup your data, as you may back up and eventually restore a corrupted database.



When performing a manual backup, the ER's database is immediately saved to the internal backup drive. From the remote server, the backup database can be retrieved via FTP, and then stored off site.



**TIP:** M86 Security recommends executing an on demand backup during the lightest period of system usage, so the Server will perform at maximum capacity.

1. Click the **Manual Backup** button in the Internal Backup/Restore Action frame to specify that you wish to back up live data to the ER Server's internal backup drive.
2. On the Confirm Backup/Restore screen, click the **Yes** button to back up the database tables and indexes.



**WARNING:** M86 Security recommends that you do not perform other functions on the ER Server until the backup is complete. The time it will take to complete the backup depends on the size of all tables being saved.

### **Perform a Remote Backup**

After executing the manual backup, a remote backup can be performed on your remote server.



**NOTE:** Before beginning this FTP process, be sure you have enough space on the remote server for storing backup data. The required space can be upwards of 200 gigabytes.

1. Log in to your FTP account.
2. Use FTP to download the ER Server's backup database to the remote server. When you are in the /backup/database/ directory, be sure to get all the \*.data files to include in your backup. You can then go to the archive directory to get all the raw logs to include in your backup.
3. Store this backup data in a safe place off the remote server. If this backup database needs to be restored, it can be uploaded to the ER Server via FTP. (See Perform a Restoration to the Server.)

## **Perform a Restoration to the ER Server**

There are two parts in performing a restoration of data to your ER Server. Part one requires data to be loaded on the remote server and then FTPed to the ER Server. Part two requires the FTPed data to be restored on the ER Server.



**NOTE:** Before restoring backup data to the ER Server, be sure you have enough space on the ER Server. Data that is restored to the ER Server will automatically include indexes.

Perform these steps on the remote server:

1. Load the backup data on your remote server.
2. Log in to your FTP account.
3. FTP the backup data to the ER Server's internal backup drive.

On the ER Server's Backup screen:

1. Click the **Manual Restore** button in the Internal Backup/Restore Action frame to specify that you wish to overwrite data on the live ER Server with data from the previous, internal backup run.
2. On the Confirm Backup/Restore screen, click the **Yes** button to restore database tables and indexes to the ER Server.



**NOTE:** The amount of time it will take to restore data to the ER Server depends on the combined size of all database tables being restored. M86 Security recommends that you do not perform other functions on the ER Server until the restoration is complete.

## Self Monitoring screen

The Self Monitoring screen displays when the Self-Monitoring option is selected from the Server menu. This screen is used for setting up and maintaining e-mail addresses of contacts who will receive automated notifications if problems occur with the network. Possible alerts include situations in which a daemon stops running, software fails to run, corrupted files are detected, or a power outage occurs.

The screenshot shows the 'Self Monitoring' dialog box within the Enterprise Reporter application. The dialog box contains the following elements:

- Header: **Self Monitoring**
- Question: **Would you like to activate self-monitoring?** with radio buttons for **YES** and **NO**.
- Instructions: **If yes, indicate who will receive the emergency e-mail notification. You may assign up to four individuals. One of them has to match with the Master Administrator email. The Master Administrator receives all messages.**
- Form fields:
  - Master Administrator's E-Mail Address:**
  - Choice one** **Send e-mail to e-mail address:**
  - Choice two** **Send e-mail to e-mail address:**
  - Choice three** **Send e-mail to e-mail address:**
  - Choice four** **Send e-mail to e-mail address:**
- Buttons: **Save**

Fig. 1:2-14 Self Monitoring screen

As the administrator of the Server, you have the option to either activate or deactivate this feature. When the self-monitoring feature is activated, an automated e-mail message is dispatched to designated recipients if the Server identifies a failed process during its hourly check for new data.

### ***View a List of Contact E-Mail Addresses***

If this feature is currently activated, the e-mail address of the Master Administrator displays on this screen, along with any other contacts set up as Choice one - four.

### ***Set up and Activate Self-Monitoring***

1. Click the radio button corresponding to **YES**.
2. Enter the **Master Administrator's E-Mail Address**.
3. In the **Send e-mail to e-mail address** fields, enter at least one e-mail address of a person authorized to receive automated notifications. This can be the same address entered in the previous field. Entries in the three remaining fields are optional.
4. If e-mail addresses were entered in any of the four optional e-mail address fields, click in the **Choice one - Choice four** checkboxes corresponding to the e-mail address(es).
5. Click the **Save** button to activate self-monitoring.

### ***Remove Recipient from E-mail Notification List***

1. To stop sending emergency notifications to an e-mail address set up in the list, remove the check mark from the checkbox corresponding to the appropriate e-mail address.
2. Click the **Save** button to remove the recipient's name from the e-mail list. The Master Administrator and any remaining e-mail addresses in the list will continue receiving notifications.

### ***Deactivate Self-Monitoring***

1. Click the radio button corresponding to **NO**.
2. Click the **Save** button to deactivate self-monitoring.

## SMTP Server Setting screen

The SMTP Server Setting screen is used for entering settings for the Simple Mail Transfer Protocol that will be used for sending email alert messages to specified administrators.

The screenshot displays the 'SMTP Server Setting' configuration window within the 'Enterprise Reporter' application. The window title is 'SMTP Server Setting'. It contains the following fields and controls:

- SMTP Server:** Text input field containing 'mail.logo.com'.
- SMTP Port:** Text input field containing '25'.
- Email queue size:** Text input field containing '50'.
- From Email Address:** Text input field containing 'alert@R3000TT64.qc.net'.
- Authentication:** Radio button controls for 'Enable' (unselected) and 'Disable' (selected).
- Username:** Empty text input field.
- Password:** Empty text input field.
- Confirm Password:** Empty text input field.
- Buttons:** 'Test Settings' and 'Apply' buttons located at the bottom right of the form area.

Fig. 1:2-15 SMTP Server Setting screen

### Enter, Edit SMTP Server Settings

1. Enter the **SMTP Server** name, for example: **mail.logo.com**.
2. By default, the **SMTP Port** number used for sending email is 25. This should be changed if the sending mail connection fails.

3. By default, the **Email queue size** is 50. This can be changed to specify the maximum number of requests that can be placed into the queue awaiting an available outbound connection.
4. In the **From Email Address** field, enter the email address of the server that will be sending alert email messages to designated administrators.
5. By default, **Authentication** is disabled. Click “Enable” if a username and password are required for logging into the SMTP server. This action activates the fields below.

Make the following entries:

- a. Enter the **Username**.
  - b. Enter the **Password** and make the same entry in the **Confirm Password** field.
6. Click **Apply** to apply your settings.

### Verify SMTP Settings

To verify that email messages can be sent to a specified address:

1. Click **Test Settings** to open the pop-up box:

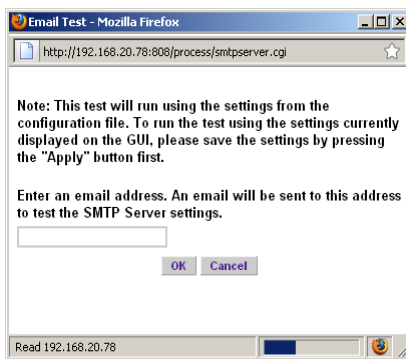


Fig. 1:2-16 SMTP Email Test box

2. Enter the email address in the pop-up box.

- Click **OK** to close the pop-up box and to process your request. If all SMTP settings are accepted, the test email should be received at the specified address.

## Server Status screen

The Server Status screen displays when the Server Status option is selected from the Server menu. This screen, which automatically refreshes itself every 10 seconds, displays the statuses of processes currently running on the Server, and provides information on the amount of space and memory used by each process.

The screenshot shows the 'Enterprise Reporter' interface with the 'Server' menu selected. The main content area displays the following information:

**Product Version:**  
Enterprise Reporter  
Version 6.0.10.1  
March 11, 2010  
Copyright 2010 M86 Security

**Server Status**

**CPU Utilization**

**CPU Load Averages:** 1.38, 1.59, 1.32

**CPU states:** 0.9%us, 0.5%sy, 0.0%ni, 96.8%id, 1.8%wa, 0.0%hi, 0.0%si, 0.0%st

**Memory:** 4151508k total, 3911804k used, 239704k free, 38204k buffers

**Swap:** 2097144k total, 84k used, 2097060k free, 2335500k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3507	dbus	20	0	2712	880	700	S	0	0.0	0:00.00	dbus-daemon
30011	root	20	0	7024	1964	1404	S	0	0.0	0:43.48	dbcontrol

**Disk drives status**

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
29931580	1730224	26680924	7%	/	
none	2075752	0	2075752	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
79473544	2477232	72959296	4%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
126951204	7982204	112640280	7%	/backup	
/dev/mapper/VG00-dblv1					
219112724	186212228	32900496	85%	/database/d1	

**NETSTAT**

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	eriii-rnd.qc.8e6.net:mysql	192.168.30.92:ums	ESTABLISHED	3667/mysqld
tcp	0	0	ERSL-121.8e6.com:mysql	ERSL-121.8e6.com:40985	ESTABLISHED	3667/mysqld
tcp	0	0	eriii-rnd.qc.8e6.net:mysql	192.168.30.92:nstp	ESTABLISHED	3667/mysqld

Fig. 1:2-17 Server Status screen

### ***View the Status of the Server***

The Product Version number of the software displays at the top of the screen, along with the date that software version was implemented. Status information displays in the following sections of this screen:

- CPU Utilization - includes CPU process data and information on the status of the top command
- Disk drives status - provides data on the status of each drive of the operating system
- NETSTAT - displays the status of a local IP address



## Secure Access screen

The Secure Access screen displays when the Secure Access option is selected from the Server menu. This screen is primarily used by M86 Security technical support representatives to perform maintenance on your Server, if your system is behind a firewall that denies access to your Server.



Fig. 1:2-18 Secure Access screen

## Activate a Port to Access the Server

1. After the administrator at the customer's site authorizes you to use a designated port to access their Server, enter that number at the **Port #** field.
2. Click the **Start** button to activate the port. This action enters the port number in the list box above, replacing the text: "No connection".



Fig. 1:2-19 Port entries

### ***Terminate a Port Connection***

1. After maintenance has been performed on the customer's Server, select the active port number from the list box by clicking on it.
2. Click the **Stop** button to terminate the port connection. This action removes the port number from the list box.

### ***Terminate All Port Connections***

If more than one port is currently active on the customer's Server and you need to terminate all port connections, click the **Stop All** button. This action removes all port numbers from the list box.

## Software Update screen

The Software Update screen displays when the Software Update option is selected from the Server menu. This screen is used for updating the Server with software updates supplied by M86 Security, and for viewing a list of software updates that are available and/or previously installed on the Server.

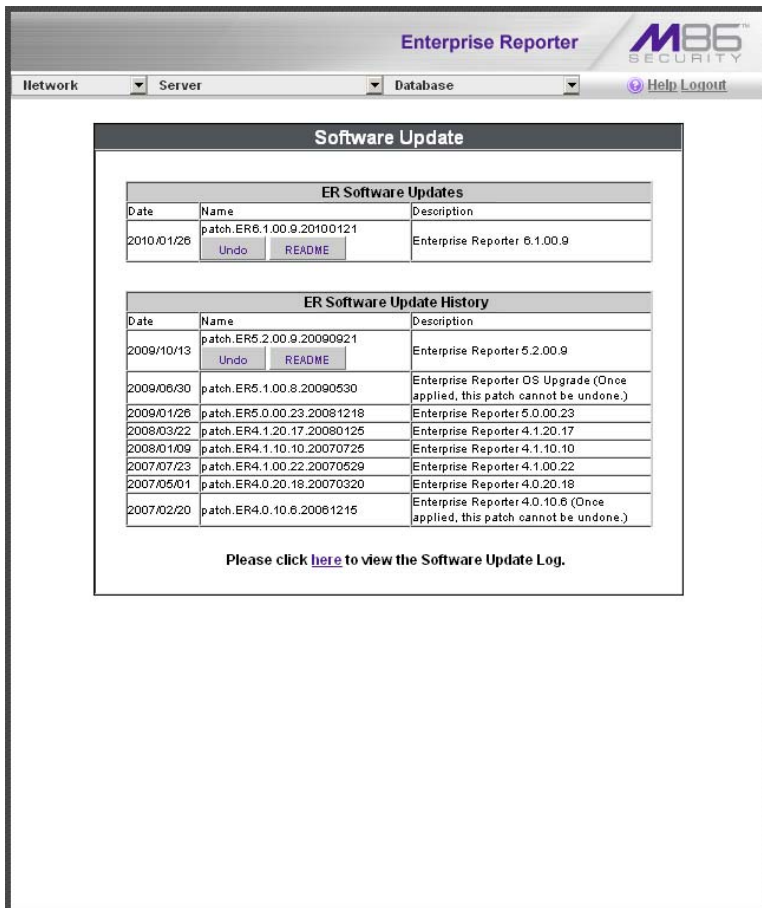


Fig. 1:2-20 Software Update screen

### ***View Installed Software Updates***

Any software update previously installed on the Server displays in the ER Software Update History frame. For each installed software update, the Date installed (YYYY/MM/DD), and software update Name and Description display.


### ***Uninstall the Most Recently Applied Software Update***


In the ER Software Update History frame, the most recently applied software update can be unapplied by clicking **Undo**. This action removes the software update from the Server.

### ***View Available Software Updates***

Any software update available for installing on the ER Server displays in the ER Software Updates frame. The following information is included for each software update: Date the software update was made available (YYYY/MM/DD), software update Name, and Description (software version number, and Prerequisite software version for installing the software update). The Apply Now and README buttons display beneath the software update name. (See Install a Software Update for information about these buttons.)

## Install a Software Update

 **WARNING:** Before installing a software update, you must shut off the Server's software by selecting the **Shutdown Software** option on the Shut Down screen. (See the Shut Down subsection under the Server menu section in this chapter.) All software updates must be installed in numerical order on your Server.

 **NOTES:** Be sure to terminate all reports that are currently running or are scheduled to run before applying a software update, and that port 8084 is open on your network.

In the ER Software Updates frame, two buttons are available: README and Apply Now.

### README:

1. Click **README** to open a pop-up box containing information about the software release:

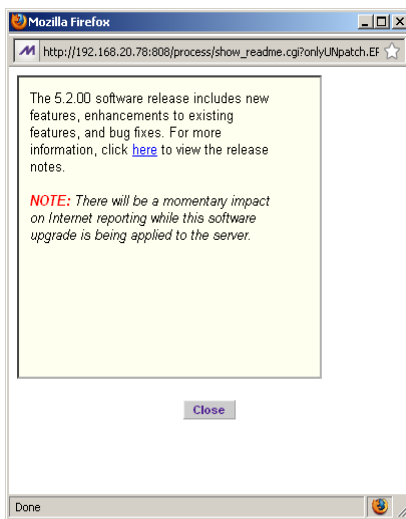


Fig. 1:2-21 Software update box

2. After reading the contents of the software release, click **Close** to close the pop-up box.

**Apply Now:**

1. Click **Apply Now** to open a dialog box containing information about the software release:

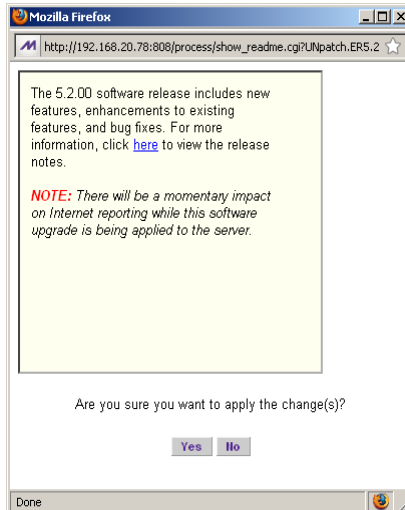


Fig. 1:2-22 Software update dialog box

2. Click **Yes** to open the EULA dialog box:

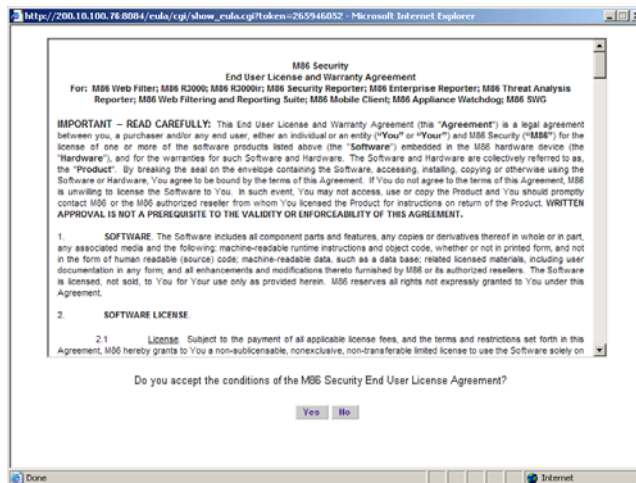


Fig. 1:2-23 EULA dialog box

3. After reading the contents of the End User License Agreement, click **Yes** if you agree to its terms. This action closes the EULA dialog box and begins the software update application process.
4. To determine whether the software update has been successfully applied, click the hyperlink (“here”) beneath the ER Software Update History frame in the Software Update screen to open the Software Update Log window:

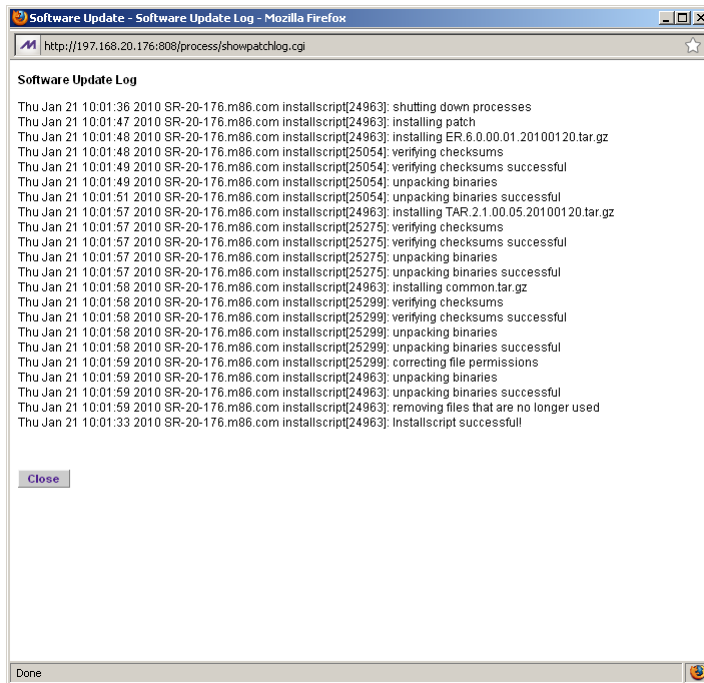



Fig. 1:2-24 Software Update Log window

5. After viewing the contents of this window, click **Close** to close this window.
6. After the software update has been successfully applied, refresh the Software Update screen by selecting Software Update from the Server pull-down menu. The soft-




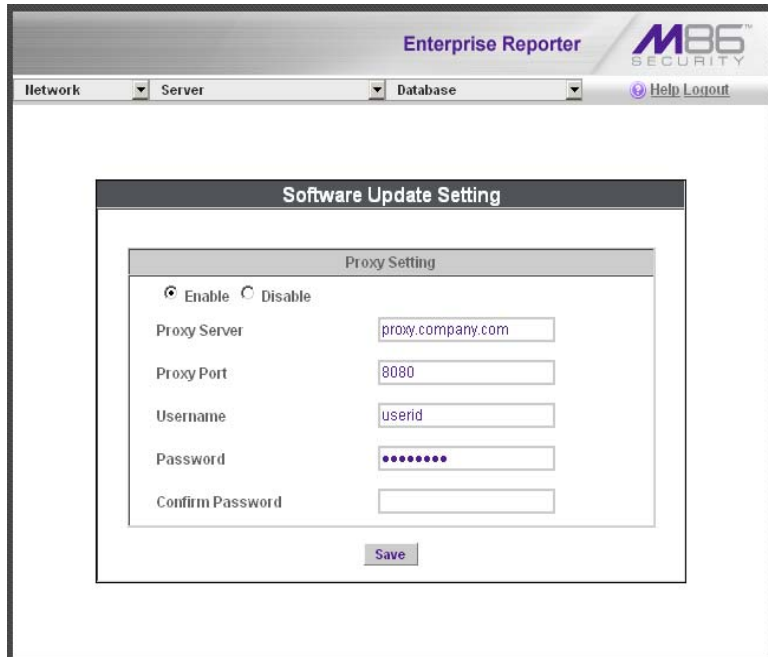
ware update details should display in the ER Software Update History frame.

 **NOTE:** After installing the software update, if a message displays that informs you to reboot the Server, you should select the **Restart Software** option on the Shut Down screen.

## Software Update Setting screen

The Software Update Setting screen displays when the Software Update Setting option is selected from the Server menu. This screen is used for configuring the ER Server to receive software updates.

 **NOTE:** This screen is only available for usage with Web Filter units set up in the Stand Alone mode. See the Synchronization sub-section in the M86 Web Filter User Guide for more information about setup modes.



The screenshot displays the 'Enterprise Reporter' web interface. At the top, there are navigation tabs for 'Network', 'Server', and 'Database', along with a 'Help Logout' link. The main content area is titled 'Software Update Setting'. Inside this area, there is a 'Proxy Setting' dialog box. The dialog box has two radio buttons: 'Enable' (which is selected) and 'Disable'. Below the radio buttons are five input fields: 'Proxy Server' (containing 'proxy.company.com'), 'Proxy Port' (containing '8080'), 'Username' (containing 'userid'), 'Password' (masked with dots), and 'Confirm Password' (empty). A 'Save' button is located at the bottom of the dialog box.

Fig. 1:2-25 Software Update Setting screen

### ***Specify Proxy Settings***

1. In the Proxy Setting frame, by default “Disable” is selected. Click “Enable” if the server is in a proxy server environment.
2. In the **Proxy Server** field, enter the host name of the proxy server.
3. In the **Proxy Port** field, enter the port number of the proxy server.
4. In the **Username** field, enter the username for the proxy account.
5. Enter the same password in the **Password** and **Confirm Password** fields.

### ***Save Settings***

Click **Save** to save your settings.

## Shut Down screen

The Shut Down screen displays when the Shut Down option is selected from the Server menu. This screen is used to restart or shut down the Server's software or hardware.

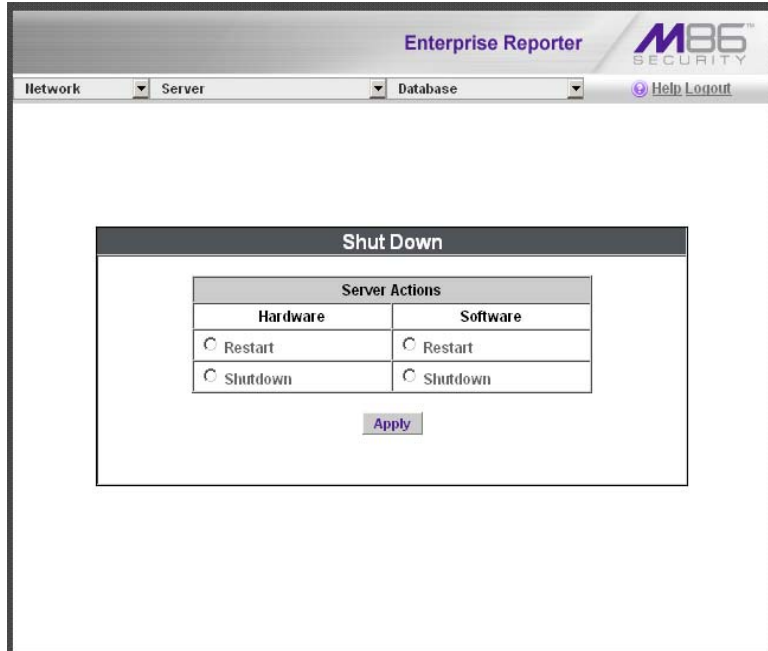


Fig. 1:2-26 Shut Down screen

### Server Action Selections

- Restart the Server's Hardware** - The Restart Hardware option should be selected if the Server box needs to be rebooted—for example, when applying certain hardware configurations. You will need to use this option if the box mode has been changed or after an IP address has been entered in the Network Settings screen. During the Hardware Restart process, files normally FTPed to the Server are routed to a problem directory in the logging device.

When the Server is running again, these files are FTPed to the Server.

- **Shut Down the Server's Hardware** - The Shutdown Hardware option should only be selected if the Server's hardware must be completely shut down—for example, if the Server box will be physically relocated. When this option is selected, the Server box shuts off, and files normally FTPed to the Server will be routed to a problem directory in the logging device. When the Server is rebooted, these files will be FTPed to the Server.
- **Restart the Server's Software** - The Restart Software option should be selected if daemons fail to run and/or the database needs to be started again. When this option is selected, the MySQL database is rebooted.
- **Shut Down the Server's Software** - The Shutdown Software option should be selected if a software update needs to be installed on the Server. When the Shutdown Software option is selected, the MySQL database shuts off and no files are FTPed to the Server.

### ***Perform a Server Action***

1. Click the radio button corresponding to the Server Action you wish to execute.
2. Click the **Apply** button to display the warning screen.
3. To proceed with your selection, click the **RESTART** or **SHUTDOWN** button on the warning screen. To change your selection, select the Shutdown window from the Server menu again to return to the Shut Down screen.



**NOTE:** *When the Restart Software or Hardware option is selected, the Server will take five to 10 minutes to reboot. After this time, you can go to another screen or log off.*

## Web Client Server Management screen

The Web Client Server Management screen displays when the Web Client Server Management option is selected from the Server menu. This screen is used for enabling specified Web Client Server features.

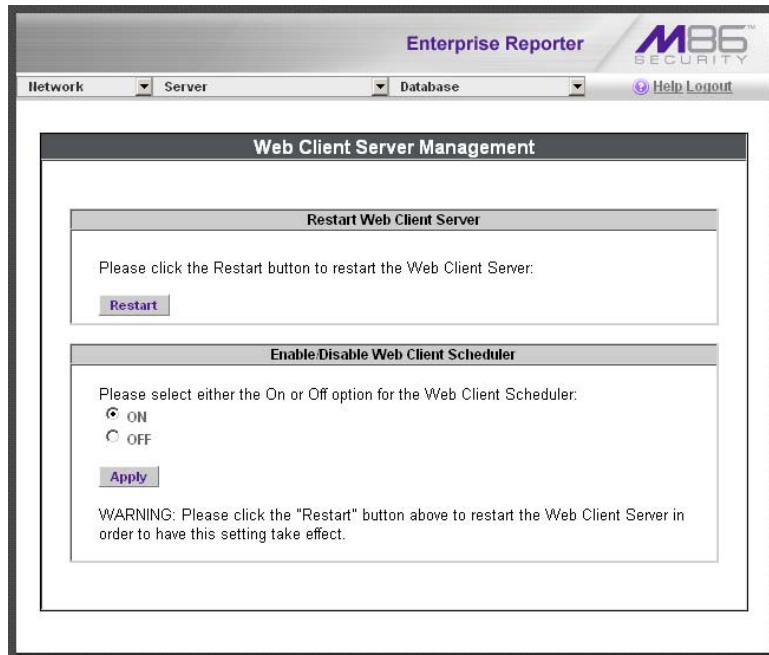


Fig. 1:2-27 Web Client Server Management screen

### **Restart the Web Client Server**

In the Restart Web Client Server frame, click **Restart** to restart the Web Client server. As a result of this action, a screen displays with the following message: “The Web Client Server will restart in a few minutes.” Click **OK** to return to the Web Client Server Management screen.

## ***Enable/Disable the Web Client Scheduler***

1. In the Enable/Disable Web Client Schedule frame, click the appropriate radio button to specify whether or not to automatically run scheduled Web Client reports:

- “ON” - Choose this option to let the Web Client automatically run scheduled reports.



**WARNING:** *Do not select this option if using the Access Client to run scheduled reports; duplicate reports will be generated.*

- “OFF” - Choose this option to use the Access Client for running scheduled reports, or if you do not want the Web Client to run scheduled reports.

2. Click **Apply**.

3. Click **Restart** to restart the Web Client Server.

## Hardware Failure Detection screen

If using an ERH, HL, or SL unit, the Hardware Failure Detection screen displays when the Hardware Failure Detection option is selected from the Server menu. This screen is used for showing the status of each drive on the RAID server.

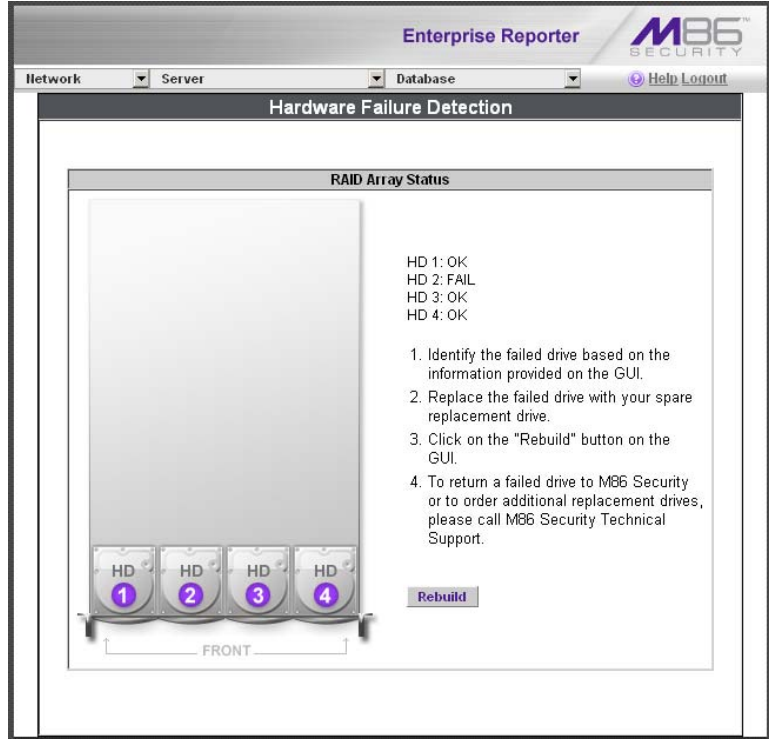


Fig. 1:2-28 Hardware Failure Detection screen

### View the Status of the Hard Drives

The current RAID Array Status displays for the four hard drives (HD 1, HD 2, HD 3, HD 4). If all hard drives are functioning without failure, the text “OK” displays for each corresponding drive number listed at the right of the screen, and no other text displays.

If any of the hard drives has failed, the message “FAIL” displays for the corresponding drive number listed at the right of the screen, and instructions for replacing the hard drive display below:

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive with your spare replacement drive.
3. Click on the “Rebuild” button on the GUI.
4. To return a failed drive to M86 or to order additional replacement drives, please call M86 Technical Support.



**NOTE:** For information on troubleshooting RAID, refer to Appendix C: RAID Maintenance and Troubleshooting.



## Consolidated ER: Consolidated Mode Setting screen

If using a consolidated ER (CER), the Consolidated Mode Setting screen displays when Consolidated Mode Setting is selected from the Server menu. This screen is used for adding, modifying, or removing information about an ER unit on the network designated to be a remote ER to this CER.

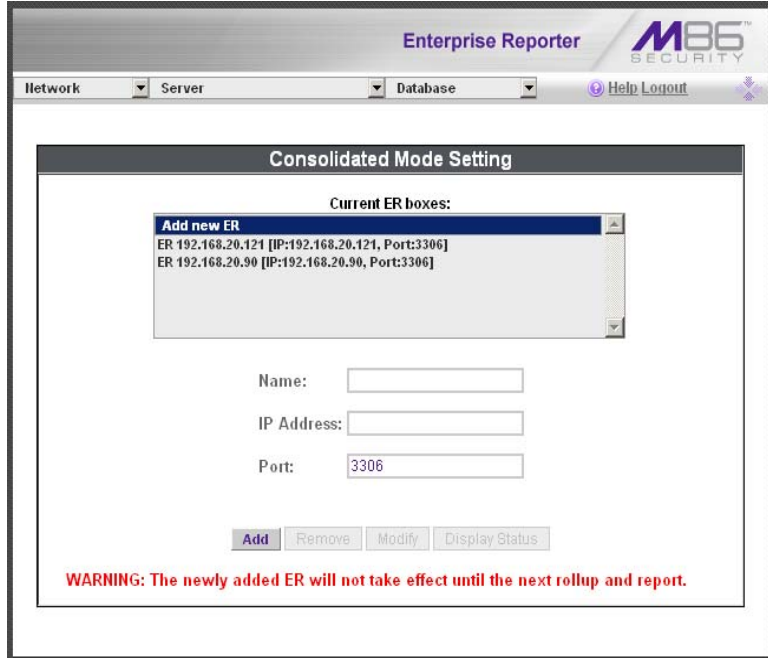


Fig. 1:2-29 Consolidated Mode Setting screen

### View Remote ER Settings

The following information displays in the Current ER boxes list box for each remote ER previously added in this screen: Name given to the remote ER, and its IP address and Port number.

### Add a Remote ER

1. By default “Add new ER” is selected in the Current ER boxes list box. If this choice is not selected, make this selection.
2. Type in a **Name** for this remote ER Server.
3. Enter the **IP Address** of the remote ER.
4. In the **Port** field, by default, 3306 displays. If necessary, this number can be changed.
5. Click **Add** to include this information for the remote ER in the Current ER boxes list box.



**NOTE:** Data from the newly-added remote ER Server will be available to this consolidated ER (CER) after the first rollup. Thereafter, automatic rollups occur every four hours, but the current day’s data will not be included. However, in the Web Client, a rollup of category groups and/or user groups can be performed on demand. See the ER Web Client User Guide for information on performing rollups on demand.

### View Current Statistics for a Remote ER

1. Select the remote ER from the Current ER boxes list box.
2. Click **Display Status** to open the ER Status pop-up box:

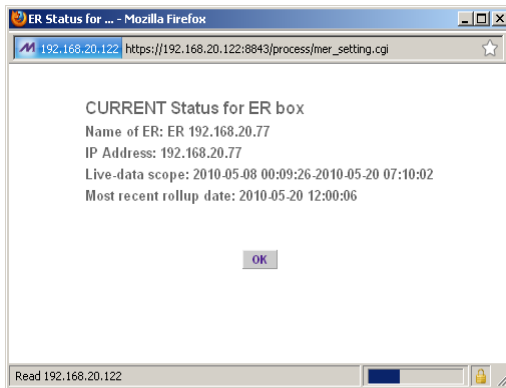


Fig. 1:2-30 ER Status pop-up window

The following information displays in this pop-up box:  
Name of ER; IP Address; Live-data-scope range (using the YYYY-MM-DD HH:MM:SS - YYYY-MM-DD HH:MM:SS format), and Most recent rollup date (using the YYYY-MM-DD HH:MM:SS format).

3. Click **OK** to close the pop-up box.

### ***Edit Settings for a Remote ER***

1. Select the remote ER from the Current ER boxes list box to display the remote ER's Name, IP Address, and Port number in the fields below.
2. Edit any of these fields.
3. Click **Modify** to save your settings.

### ***Remove a Remote ER from the Consolidated ER***

1. Select the remote ER from the Current ER boxes list box to display the remote ER's Name, IP Address, and Port number in the fields below.
2. Click **Remove** to display the page that asks if you wish to remove the ER you just added to the list box.



**TIP:** Click **NO** to return to the Consolidated Mode screen.

3. Click **Yes** to return to the Consolidated Mode screen with the ER removed from the list box.

## Database Menu

---

The Database pull-down menu includes options for configuring the database. These options are: IP.ID, Username Display Setting, Elapsed Time, Page Definition, Tools, Expiration, Optional Features, and User Group Import.



**NOTE:** *On a consolidated ER (CER), only the following options are available: Tools, Expiration, Optional Features, and User Group Import. Some of these screens differ on the CER.*

## User Name Identification screen

The User Name Identification screen displays when the IP.ID option is selected from the Database menu. This screen is used for configuring the Server to identify users based on the IP addresses of their machines, their usernames, and/or their machine names. Information set up on this screen is used by the Client when logging a user's Internet activity.



**NOTE:** *This option is not available in a consolidated ER.*


The screenshot shows the 'User Name Identification' configuration page in the Enterprise Reporter interface. At the top, there are navigation tabs for 'Network', 'Server', and 'Database', along with a 'Help Logout' link. The main content area is titled 'User Name Identification' and contains the following elements:

- Radio buttons for 'Enable' (selected) and 'Disable'.
- A section header 'IP.ID (Microsoft Username Lookup)'.
- Two checked checkboxes: 'IP.ID' and 'Static IP assignment'.
- Text: 'Click Update to instantly create a table of Static IPs and Machine Names.' with an 'Update' button.
- A section header 'IPs, Machines, Usernames to ignore'.
- Text: 'Please enter the IP, Machine & Username you wish to ignore below: (One Name Per Line)'.
- Three text input fields:
  - 'IP to ignore:' containing '200.10.160.11' and '200.10.160.53'.
  - 'Machine to ignore:' containing 'admin-edot'.
  - 'Username to ignore:' containing 'emartin' and 'jchaire'.
- A 'Save' button at the bottom.


Fig. 1:2-31 User Name Identification screen with IP.ID activated


As the administrator of the Server, you have the option to either enable or disable this feature for logging users' activities by usernames, machine names, and/or IP addresses of machines.

## WARNINGS

 *The ER will generate NetBIOS requests outside the network if IP.ID is activated **and** if no segment settings have been specified in the configuration of the Web access logging device—causing it to log external traffic. To resolve this issue, the Web access logging device should be modified to log activity only within the network. If a firewall is used, it should be set up to prevent logging NetBIOS requests outside the network.*

**NOTE:** *Depending on the type of Web access logging device you are using, there may not be a configuration parameter for segment settings.*

 *Be sure the time zone specified for the ER is the same for each Web access logging device the ER uses. Failure in executing this setup will cause inconsistencies when users' logging times are reported, especially if IP.ID is activated. If multiple Web access logging devices are used, be sure to identify the subnets assigned to each of these devices, as users cannot be tracked solely by IP address.*

 *If using IP.ID, note that user login times are established for set periods of 15 minutes, and if more than one user logs onto the same machine during that time period, the activity on that machine will be identified with the first user who logged onto that machine. For example, the first user logs on a machine for three minutes and then logs off. The second user logs on the same machine for 11 minutes and then logs off. The first user logs back on that machine for 16 minutes. All 30 minutes are logged as the first user's activity.*

## **View the User Name Identification screen**

If user name identification is enabled, specified IP.ID criteria displays, and IP, Machine, and Username frames will be populated if entries were previously made in them.



**NOTE:** *If this feature is disabled, checkboxes in the IP.ID (Microsoft Username Lookup) section display greyed-out.*

## **Configure the Server to Log User Activity**

1. In the area above the IP.ID (Microsoft Username Lookup) section of the screen, click the radio button corresponding to **Enable**. This action opens an alert box informing you that if usernames are enabled, these usernames will overwrite those that are being imported from the shadow log.
2. Click **OK** to close the alert box, and to activate the IP.ID and Static IP assignment checkboxes.
3. in the IP.ID (Microsoft Username Lookup) section of the screen, select one or both of the following options by clicking in the designated checkbox(es):
  - **IP.ID** - this option logs a user's activity by username (login ID).
  - **Static IP assignment** - this option logs a user's activity by the IP address of the machine used. When selecting this option, the Update button becomes activated.
    - a. Click the **Update** button to automatically generate a table of static IP addresses and machine names. After this table is created, the message screen displays to confirm the successful execution of this task.
    - b. Click the **Back** button to return to the User Name Identification screen.

4. In the IP/Machine/Username to ignore list boxes, enter all IP addresses, machine names, and/or usernames the Server should disregard when identifying users. Each entry should be made in a separate row.
5. After making all necessary entries on this screen, click the **Save** button.

### ***Deactivate User Name Identification***

1. Click the radio button corresponding to **Disable**.
2. Click the **Save** button.



## Username Display Setting screen

This Username Display Setting screen displays when the Username Display Setting option is selected from the Database menu. This screen is used for configuring the username format imported from raw logs and customizing the username format that displays in reports.



**NOTE:** This option is not available in a consolidated ER.

Enterprise Reporter **M86** SECURITY

Network Server Database Help Logout

### Username Display Setting

**Current Username Display Setting**

The current display name format is:

**Modify Username Display Setting**

Please SELECT the username in the raw log from the following fields:

Available Fields:

Domain Name  
Organization Name  
Department Name  
User Name

Please select how you want the username displayed on the ER report and click "Apply":

Raw Log Fields:

Display username:

**WARNING: After applying or updating a username format, please re-run the User Group Import from the Admin console. This ensures the new user group patterns can be used in drill down reports for these user groups.**

Fig. 1:2-32 Username Display Setting screen

## View the Current Username Display Setting

In the Current Username Display Setting frame, the current username format displays—if previously entered in the Display username field and saved on this screen.

## Modify the Username Display Setting

In the Modify Username Display Setting frame, make selections from list boxes and apply results for the new username format to be displayed in the report.

1. By default, the following choices display in the Available Fields list box: Domain Name, Organization Name, Department Name, User Name. Make a selection from this list for the first field displayed in your server console and raw logs that you wish to include in the username format in the report.
2. Click **Add** to include this selection in the Raw Log Fields list box below.



**NOTE:** Follow steps 1 and 2 for each consecutive field to be added to the Raw Log Fields list box.



**TIP:** Click the Reset button on this screen at any time to revert to the default settings.



**WARNING:** It is important to select the correct fields from this list, in the order in which they appear in your server console. For example, if the username format on the console is Domain Name\Department Name\User Name, and only User Name and Department Name are selected from the Available Fields list box—in that order—the report will display information in the wrong order. In this example, if the Domain Name is LOGO, the Department Name is Admin, and the User Name is JSmith, the report will show JSmith\Admin, instead of LOGO\Admin\JSmith.

3. In the Raw Log Fields list box, select the first field to be displayed in the username format on the report.

4. Click **Add** to include your selection in the Display username field below.



**NOTE:** Follow steps 3 and 4 for each field to be added to the Display username field below. Each additional selection added to the display name is preceded by a backslash ( \ ).

5. Click **Apply** to save your entries and to display the new username format in the Current Username Display Setting frame.



**NOTE:** Changes made to username display settings in this screen will not be effective until the next day's reports are generated.



**WARNING:** After modifying a username format, be sure to import users and groups using the User Group Import screen. See the User Group Import screen for information on importing user groups.

## Page View Elapsed Time screen

The Page View Elapsed Time screen displays when the Elapsed Time option is selected from the Database menu. This screen is used for establishing the value—amount of time—that will be used when tracking the length of a user's stay at a given Web site, and the number of times the user accesses that site.



**NOTE:** This option is not available in a consolidated ER.

The screenshot shows the 'Page View Elapsed Time' configuration screen. At the top, there is a navigation bar with 'Enterprise Reporter' and the 'M86 SECURITY' logo. Below this are dropdown menus for 'Network', 'Server', and 'Database', and links for 'Help' and 'Logout'. The main content area features a dark header with the title 'Page View Elapsed Time'. Below the header is a form with a text input field labeled 'Elapse Time' containing the value '10', followed by the text 'seconds'. A 'Save' button is positioned below the input field.

Fig. 1:2-33 Page View Elapsed Time screen

### ***Establish the Unit of Elapsed Time for Page Views***

1. In the **Elapse Time** field, enter the number of seconds that will be used as the value when tracking a user's visit to a Web site.
2. Click the **Save** button.

## ***Elapsed Time Rules***

Each time a user on the network accesses a Web site, this activity is logged as one or more visit(s) to that site. The amount of time a user spends on that site and the number of times he/she accesses that site is tracked according to the following rules:

- A user will be logged as having visited a Web site one time if the amount of time spent on any pages at that site is equivalent to the value entered at the Elapse Time field, or less than that value.

For example, if the value entered at the Elapse Time field is 10 seconds, and if the user is at a site between one to 10 seconds—on the same page or on any other page within the same site—the user’s activity will be tracked as one visit to that Web site.

- Each time the user exceeds the value entered at the Elapse Time field, the user will be tracked as having visited the site an additional time.

For example, if the value entered at the Elapse Time field is 10 seconds and the user remains at a Web site for 12 seconds, two visits to that site will be logged for him/her.

- Each session at a Web site is tracked as one or more visit(s), depending on the duration of the session. A session is defined as a user’s activity at a site that begins when the user accesses the site and ends when the user exits the site.

For example, if the value entered at the Elapse Time field is 10 seconds and the user spends five seconds on a Web site, then exits, then returns to the same site for another 15 seconds, the user will have two sessions or three visits to that site logged for him/her (5 seconds = 1 visit, 15 seconds = 2 visits, for a total of 3 visits).

## Page Definition screen

The Page Definition screen displays when the Page Definition option is selected from the Database menu. This screen is used for specifying the types of pages to be included in the detail report for Page searches.



**NOTE:** This option is not available in a consolidated ER.

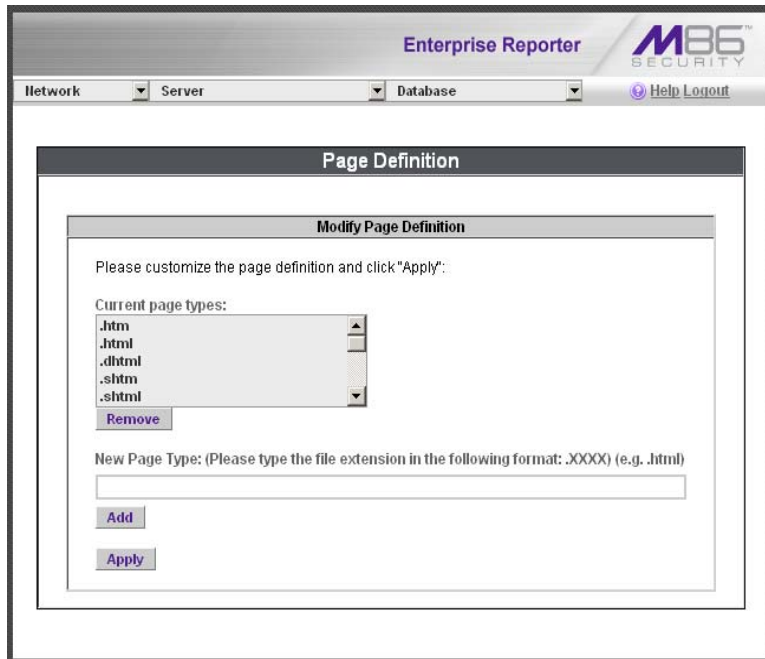


Fig. 1:2-34 Page Definition screen

### View the Current Page Types

The Current page types list box contains the extensions of page types to be included in the detail report.

### ***Remove a Page Type***

To remove a page type from the detail report:

1. Select the page extension from the Current page types list box.
2. Click **Remove**.
3. Click **Apply**.

### ***Add a Page Type***

To add a page type in the detail report:

1. Enter the **New Page Type** extension.
2. Click **Add** to include the extension in the Current page types list box.
3. Click **Apply**.

## Tools screen

The Tools screen displays when the Tools option is selected from the Database menu. This screen is used for viewing reports and logs to help you troubleshoot problems with the Client application.

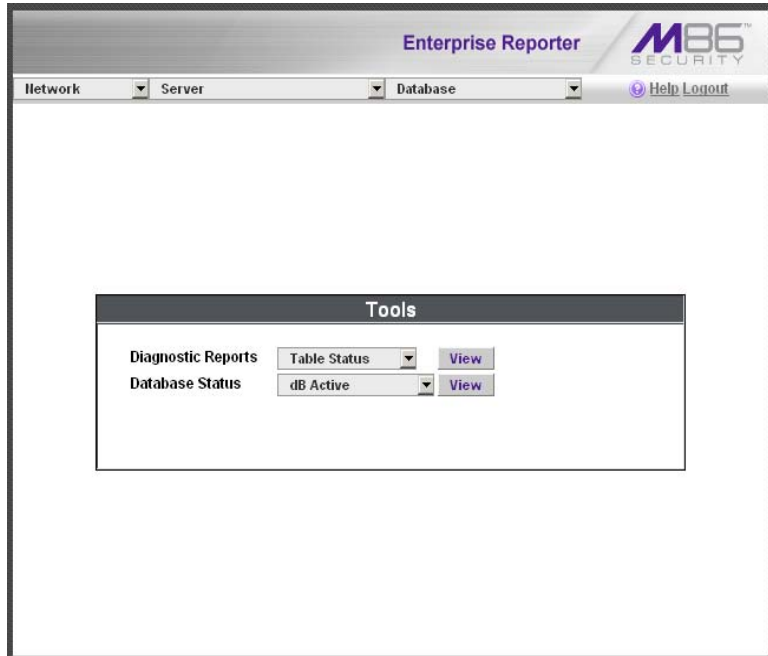


Fig. 1:2-35 Tools screen

The following options are available on this screen:

- View Diagnostic Reports
- View Database Status Logs



## ***View Diagnostic Reports***

1. Choose a report from the pull-down menu (Table Status, Process List, Full Process List, Tables, or Daily Summary).
2. Click the **View** button to view the selected diagnostic report in a pop-up window:
  - **Table Status** - This report contains a list of Client table names, and columns of statistics on each table, such as type, size, number of rows, and time created and updated.
  - **Process List** - This report shows a list of current SQL queries in the database, in an abbreviated format.
  - **Full Process List** - This report shows a list of current SQL queries in the database, in the full format that includes all columns of data.
  - **Tables** - This report contains a list of the names of tables currently in the database.
  - **Daily Summary** - This report shows the date range of summary tables currently in the database.
3. Click the “X” in the upper right corner of the pop-up window to close the window.

## ***View Database Status Logs***

1. Choose a database status log from the pull-down menu.
2. Click the **View** button to view the selected database status log in a pop-up window:
  - **db Active** - This log indicates when client tables were last updated with hits\_objects and hits\_pages.
  - **db Backup** - This log provides information about the MySQL backup/restore operation.
  - **db Control** - This log shows a list of actions performed by the ER process when processing log files.

- **db Expiration** - This log includes information about expiring data on the Server.
- **db Expire Summary** - This log provides a list of data expiration from summary tables.
- **db Identify** - This log provides information about the Server's action of obtaining user/machine names from name log files and populating the database with these names.
- **db Ipgroups** - This log lists individual and group IP records that were added to—and deleted from—the client group lookup table.
- **db Logloader** - This log provides information about log file parsing and the number of valid and invalid records that are processed.
- **db Nbtlookup** - This log provides a list of user/machine IP addresses from the NetBIOS lookup.
- **db Split** - This log contains information pertaining to the formation of the hits\_objects/hits\_pages tables.
- **db Staticip** - This log provides information about settings on the server for the static IP assignment option.
- **db Summary** - This log shows a summarization of activities from the dbsummary database tool.
- **db Support** - This log includes a list of temporary tables that were created for the formation of the hits tables.
- **db Tool** - This log shows information about system checks performed on disk usage, free memory, unprocessed files, and daemons.
- **db Traffic** - This log provides information about the daily traffic table.
- **File Watch Log** - This log shows a list of records that were imported from one machine to another.

- **Software Update Log** - This log gives information about applied software updates.
  - **MYSQL Log** - This log provides information pertaining to the MySQL server.
  - **Error Entry - Web Filter** - This log displays a list of Web Filter query errors.
3. Click the “X” in the upper right corner of the pop-up window to close the window.

## Expiration screen

The Expiration screen displays when the Expiration option is selected from the Database menu. This screen shows statistics on the amount of data currently stored on the Server box, and provides an estimated date when that data will expire. By reviewing the current database disk space utilization and the average number of daily hits on your Server, adjustments can be made to the number of weeks of live and archive data you wish to store in the future before that data expires.

The screenshot shows the 'Expiration' screen within the Enterprise Reporter interface. The top navigation bar includes 'Enterprise Reporter' and the M86 SECURITY logo. Below the navigation bar are dropdown menus for 'Network', 'Server', and 'Database', along with 'Help Logout' links. The main content area is titled 'Expiration' and displays the following information:

**Status as of 2009-12-23 01:27:34**

Date scope for total data	2009-12-11 00:09:26 - 2009-12-23 00:09:44
Total number of week(s) stored	2 week(s)
Current live data (yearweekno/date scope)	200949 - 200951 2009-12-11 00:09:26 - 2009-12-23 00:09:44
Total number of live week(s)	2 week(s)
Current archive data (yearweekno/date scope)	0 - 0 0 - 0
Total number of archive week(s)	0 week(s)
Database disk space utilization (used database space/total database space)	3.44 % (1.73/50.33 Gbytes)
Target percentage of live data	100 %
Last 8 weeks hits/day average	112849
Estimated total week(s) of live data	226 week(s)
Estimated total week(s) of archive data	0 week(s)
Estimated number of week(s) until next expiration	49 week(s)

**Change Settings**

Hits/day	112849
Percentage of live data	100 %
<input type="button" value="Calculate"/>	
Estimated total week(s) of live data	<input type="text"/> week(s)
Estimated total week(s) of archive data	<input type="text"/> week(s)
<input type="button" value="Save"/>	

Fig. 1:2-36 Expiration screen



**NOTES:** *On a consolidated ER (CER), several of the statistics shown in a standard ER are not included since this information is not pertinent to the CER.*

*Though the database is backed up automatically each day, under certain circumstances you may need to perform a manual backup to the internal backup drive, and then save this data off site. (See the Server Menu Backup screen section for information on establishing backup procedures, and backing up and restoring data on the ER Server.)*

### **Expiration Screen Terminology**

The following terminology is used on the Expiration screen:

- **Live** - pertains to indexed data on the hard drive of the Server for the most recent weeks—the period designated as “live.” Indexed data includes pages and objects that were accessed by users on the Internet, as well as the indexes for these items.

When setting up the Server to store data, M86 Security recommends that you allocate the highest percentage possible for live data storage, since reports run faster if indexes are available for pages and objects.

If your Server is set up to store live data only (100 percent live data), you will be able to store less data than if you store both live and archive data, since indexes require additional storage space.

- **Archive** - pertains to non-indexed data on the hard drive of the Server for the oldest weeks—the period designated as “archive.” Non-indexed data might include pages and/or objects that were accessed by users on the Internet.

Since archive data contain no indexes, they occupy less space on the Server than live data—which include indexes and pages/objects. However, reports generated for periods of time with archive data take longer to process since indexes are not included for that data.

- **Expire** - pertains to the action of dropping data from the Server when there is no room left on the hard drive for additional storage. When the hard drive reaches its maximum data storage capacity, indexes from the oldest week of data stored on the Server are dropped, or “expired” from the Server. Thereafter, when more space is needed on the Server, the oldest week of non-indexed data “expires.”

### ***Expiration Rules***

The administrator of the Server specifies the number of weeks of data that will be stored on the Server, based on the storage capacity of the hard drive, and the number of hits on the Server. After inputting the percentage of live data to be stored, the Server translates that figure into the equivalent of weekly time periods for live and/or archive data storage.

When the Server reaches the maximum number of weeks allocated for live data storage, the oldest week of live data stored on the Server attains an archive data status. In attaining an archive data status, the index for that week of data is dropped from the database tables.

When the Server reaches its maximum number of weeks allocated for archive data storage, the oldest week of non-indexed data stored on the Server is automatically dropped (expired) from the database.

Once data expires, it cannot be recovered.

## View Data Storage Statistics

In the Status section of this screen, the date and time of the last database expiration displays in the Status bar. The date displays in the YYYY-MM-DD format, and the time displays in military time (01-24 hours) using the HH:MM:SS time format.

The following data that displays is current as of the most recent database expiration run:

- **Data scope for total data** - the date and time range of all live and archive data currently stored on the Server. The date displays in the YYYY-MM-DD format, and the time displays in military time (01-24 hours) using the HH:MM:SS time format.
- **Total number of week(s) stored** - the number of weeks represented in the total data date scope.
- **Current live data (yearweekno/date scope)** - the range of dates and times of live data currently stored on the Server.

The first line displays the range of year(s) and weeks in the YYYYWW format, where “Y” represents the year, and “W” represents the week number in that year (01-52).

The second line displays the first date and time in the range of live data currently stored on the Server. The date displays in the YYYY-MM-DD format, and the time displays in military time (1-24 hours) using the HH:MM:SS time format.

The third line displays the last date and time in the range of live data currently stored on the Server, using the same format as in the second line of data.



**NOTE:** *This field does not display on a consolidated ER.*

- **Total number of live week(s)** - the number of weeks represented in the live data date scope.



**NOTE:** *This field does not display on a consolidated ER.*

- **Current archive data (yearweekno/date scope)** - the range of dates and times of archive data currently stored on the Server.

The first line displays the range of year(s) and weeks in the YYYYWW format, where “Y” represents the year, and “W” represents the week number in that year (01-52).

The second line displays the first date and time in the range of archive data currently stored on the Server. The date displays in the YYYY-MM-DD format, and the time displays in military time (1-24 hours) using the HH:MM:SS time format.

The third line displays the last date and time in the range of archive data currently stored on the Server, using the same format as in the second line of data.



**NOTE:** *This field does not display on a consolidated ER.*

- **Total number of archive week(s)** - the number of weeks represented in the archive data date scope.



**NOTE:** *This field does not display on a consolidated ER.*

- **Database disk space utilization** - the percentage of space currently being used on the hard drive for both live and archive data. If a high percentage displays, you may want to expire data in the near term (see Change Data Storage Settings).



**NOTE:** *Archive data is not applicable to a consolidated ER.*

- **(used database space/total database space)** - the amount of space in Gigabytes currently being used on the hard drive for both live and archive data, and the total amount of space in Gigabytes (Gbytes) on the hard drive allocated to database storage.



**NOTE:** *Archive data is not applicable to a consolidated ER.*



- **Average disk usage per day** - this field only displays on the consolidated ER and shows the average percentage of disk space used each day.
- **Target percentage of live data** - the percentage of live data to be stored on the Server. If this figure is 100, only live data will be stored. If this figure is less than 100, the remaining percentage to be stored will be archive data.

The percentage that displays can be changed by entering and saving a different figure in the Percentage of live data field in the Change Settings section of this screen.



**NOTE:** This field does not display on a consolidated ER.

- **Last 8 weeks hits/day average** - the average number of hits on the Server per day, based on the last eight weeks of data stored on the Server.



**NOTE:** This field does not display on a consolidated ER.

The following data that displays is current as of the last changes made in the Change Settings section of the screen:

- **Estimated total week(s) of live data** - the number of weeks of live data the Server will store, based on your specifications. This number is affected by the hits/day on the Server, and the maximum number of weeks of data the Server is able to hold.

The number of weeks of live data to be stored can be changed by making a new entry in the Percentage of live data field in the Change Settings section of this screen, and saving the result of your calculations that displays below in the Estimated total week(s) of live data field.



**NOTE:** This field does not display on a consolidated ER.

- **Estimated total week(s) of archive data** - the number of weeks of archive data the Server will store, based on

your specifications. This number is affected by the hits/day on the Server, and the maximum number of weeks of data the Server is able to hold.

The number of weeks of archive data to be stored can be changed by making a new entry in the Percentage of live data field in the Change Settings section of this screen, and saving the result of your calculations that displays below in the Estimated total week(s) of archive data field.



**NOTE:** *This field does not display on a consolidated ER.*

- **Estimated number of week(s) until next expiration** - the number of weeks from this week that data on the Server will expire.

### ***Change Data Storage Settings***

The Change Settings section of the screen is used for updating the amount of data that will be stored on the Server box in the future. By making an entry in this section of the screen, you dictate how data on the box will expire.

1. At the Hits/day field, the number of hits on the Server per day displays. This is the same figure that displays in the Last 8 weeks hits/day average field in the Status section above.

On a consolidated ER, enter the **Hits/day**.

2. In the **Percentage of live data** field, enter a figure for the percentage of data you wish to be stored as live data on the box. If you want all data to be live data only, enter 100.



**NOTE:** *This field does not display on a consolidated ER.*

3. Click the **Calculate** button to display the following results:

- On a standard ER, the Estimated total week(s) of live data and Estimated total week(s) of archive data display in the fields beneath the Calculate button.
- On a consolidated ER, the Estimated weeks to store data displays in the field above the Calculate button.

After viewing your results, you can adjust the number of weeks that data will be saved on the Server, if necessary. To do so, follow steps 1 - 3 again.

4. On a consolidated ER, enter the **Weeks desired to keep data**.
5. After reviewing and accepting the final calculation(s), click the **Save** button. As a result of your entries, the following occurs on a standard ER:
  - the figure saved in the Percentage of live data field displays in the Target percentage of live data field in the Status section
  - the figures displayed in the Estimated total week(s) of live/archive data fields display in the Estimated total week(s) of live/archive data fields in the Status section
  - the Estimated number of week(s) until next expiration field may display a new figure, based on the new settings you saved.

**When the next database expiration runs, all other fields in the Status section will reflect the new calculations.**



**TIP:** M86 Security recommends that you set up your Server to store more live data than archive data for the benefit of administrators and sub-administrators who generate reports via the Client application. Report processing times are slower when generating reports that include non-indexed data.

*If your Server is set up to store only live data, you will be able to store less data than if you store both live and archive data, since indexes require additional storage space.*



**NOTE:** See Appendix A: Evaluation Mode for information about viewing the Expiration screen in the evaluation mode.

## Optional Features screen

The Optional Features screen displays when Optional Features is selected from the Database menu. This screen is used for specifying any of the following options to be available in the Web Client when generating specified types of reports: Search String Reporting, Block Request Count, Blocked Searched Keywords, Wall Clock Time, Object Count. This screen also is used for enabling and configuring the password security feature to be used for the Administrator console and/or Web Client (see Fig. 1-2:37).



**NOTES:** *Optional features can be enabled or disabled at any time. On a consolidated ER, the Search String Reporting and Object Count options are not available.*

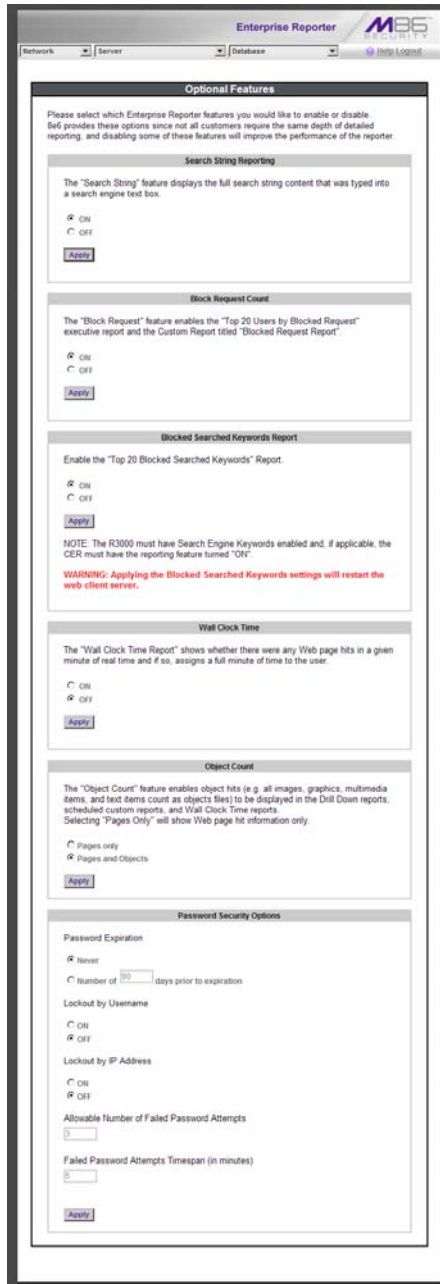


Fig. 1:2-37 Optional Features screen

## ***Enable Search String Reporting***

If Search String Reporting is enabled, detail drill down reports display the full search string content typed into a search engine text box for search sites such as Google, Bing, Yahoo!, MSN, AOL, Ask.com, YouTube.com, and MySpace.com.



**NOTE:** *This feature is not available on a consolidated ER.*

1. Click the radio button corresponding to “ON” to let search string entries display in drill down reports.
2. Click **Apply** to apply your setting.

## ***Enable Block Request Count***

If Block Request Count is enabled, the Top 20 Users by Blocked Request Executive Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request Executive Report selection available in an administrator’s Executive Reports menu.
2. Click **Apply** to apply your setting.



**NOTE:** *Since Executive Reports are processed each night, any changes made to settings today will not effective until the following day.*

## ***Enable Blocked Searched Keywords***

If Blocked Searched Keywords is enabled, the Top 20 Blocked Searched Keywords Executive Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request Executive Report selection available in an administrator’s Executive Reports menu.

2. Click **Apply** to apply your setting.



**WARNING:** Applying this setting restarts the Web Client server.



**NOTE:** Since Executive Reports are processed each night, any changes made to settings today will not be effective until the following day.

### **Enable Wall Clock Time**

If Wall Clock Time is enabled, Wall Clock Time Reports can be generated by the administrator. These reports use the Wall Clock Time algorithm to calculate the amount of time an end user spent accessing a given page or object—disregarding the number of seconds from each hit and counting each unique minute of Web time as one minute. Using this algorithm, an end user could never have more than 24 hours of Web time within a given 24-hour period.

1. Click the radio button corresponding to “ON” to make the Wall Clock Time Report selection available in an administrator’s Custom Reports menu.
2. Click **Apply** to apply your setting.



**NOTE:** Since Wall Clock Time reports are processed each night, any changes made to settings today will not be effective until the following day.

### **Enable Page and/or Object Count**

In the Object Count frame, indicate whether drill down, Wall Clock Time, and scheduled custom reports will include Web page hits only, or both Web page and object hits. Objects include images, graphics, multimedia items, and text item object files.



**NOTE:** This feature is not available on a consolidated ER.



**WARNING:** If “Pages only” is selected, **all** records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes (“0”) will display for object activity in generated reports.

1. Select one of two radio buttons to specify the type of hits to be included in drill down, Wall Clock Time, and scheduled custom reports:
  - “Pages only” - Choose this option to include *only* Web page hits in reports.
  - “Pages and Objects” - Choose this option to include *both* Web page and object hits in reports.
2. Click **Apply** to apply your setting.

### ***Enable, Configure Password Security Option***

In the Password Security Options frame, passwords for accessing the Administrator console or Web Client can be set to expire after a specified number of days, and/or lock out the user from accessing the Administrator console and Web Client after a specified number of failed password entry attempts within a defined interval of time.

1. Enable any of the following options:
  - At the **Password Expiration** field, click the radio button corresponding to either password expiration option:
    - **Never** - Choose this option if passwords will be set to never expire.
    - **Number of ‘x’ days prior to expiration** - Choose this option if password will be set to expire after ‘x’ number of days (in which ‘x’ represents the number of days the password will be valid).



**NOTES:** *The maximum number of days that can be entered is 365.*



*If a user's password has expired, when he/she enters his/her User Name and Password in the login screen and clicks Login, he/she will be prompted to re-enter his/her User Name and enter a new password in the Password and Confirm Password fields.*

- At the **Lockout by Username** field, click the radio button corresponding to either of the following options:
  - **ON** - Choose this option to lock out the user by username if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts field—within the interval defined in the Failed Password Attempts Timespan (in minutes) field.
  - **OFF** - Choose this option if the user will not be locked out by username after entering the incorrect password.
- At the **Lockout by IP Address** field, click the radio button corresponding to either of the following options:
  - **ON** - Choose this option to lock out the user by IP address if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts field—within the interval defined in the Failed Password Attempts Timespan (in minutes) field.
  - **OFF** - Choose this option if the user will not be locked out by IP address after entering the incorrect password.
- **Allowable Number of Failed Password Attempts** - With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of times a user can enter an incorrect password during the interval defined in the Failed Password Attempts Timespan (in minutes) field before being locked out of the ER application.



**NOTE:** *The maximum number of failed attempts that can be entered is 10.*

- **Failed Password Attempts Timespan (in minutes)** - With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of minutes that defines the interval in which a user can enter an incorrect password—as specified in the Allowable Number of Failed Password Attempts field—before being locked out of the ER application.



**NOTE:** *The maximum number of minutes that can be entered is 1440.*

2. Click **Apply** to apply your settings.

## User Group Import screen

The User Group Import screen displays when the User Group Import option is selected from the Database menu. This screen is used for specifying Web Filter servers to send LDAP user group membership information to this ER Server, for performing a user group import on demand, and for viewing on demand user group import criteria.

The screenshot shows the 'Enterprise Reporter' interface with a navigation bar containing 'Network', 'Server', and 'Database' menus. The main content area is titled 'User Group Import' and contains the following elements:

- Four input fields for 'Web Filter IP' addresses. The first field contains '192.168.20.17' and has a checked checkbox labeled 'Import from this Web Filter'. The other three fields are empty and have unchecked checkboxes.
- A button labeled 'More Web Filters'.
- A warning message: 'Importing user groups may take a long time depending on the number of Web Filters and the number of users for each Web Filter.'
- An 'Import Now' button.
- A section titled 'Current Status for User Group Import:' containing a box with the following text:
  - Importing groups from Web Filter 192.168.20.17 .....
  - Running dbipgroups .....
  - Importing user groups finished successfully.

Fig. 1:2-38 User Group Import screen



**WARNING:** Be sure to import users and user groups whenever modifications are made to usernames in the Username Display Setting screen. See the Username Display Setting screen for information on modifying usernames.

### **Import User Groups**



**NOTE:** Web Filter IP fields are populated by default if one or more Web Filter servers are connected to this ER server.

1. Specify the **Web Filter IP** address of each Web Filter to send LDAP user group membership data to this ER.
2. Click the checkbox corresponding to “Import from this Web Filter”.



**NOTE:** If additional Web Filter servers need to be specified, click **More Web Filters** to display the next four sets of entry fields.

3. After specifying all Web Filter servers from which to import user group data, click **Import Now** to begin the data importation process. The status of this process displays in the Current Status for User Group Import box that opens at the bottom of this screen when the Import Now button is clicked.



**NOTE:** User groups will be imported in the exact format defined on the Web Filter.

# TECHNICAL SUPPORT / PRODUCT WARRANTIES

## Technical Support

For technical support, visit M86 Security's Technical Support Web page at <http://www.m86security.com/support/> or contact us by phone, by email, or in writing.

### *Hours*

Regular office hours are from Monday through Friday, 8 a.m. to 5 p.m. PST.

After hours support is available for emergency issues only. Requests for assistance are routed to a senior-level technician through our forwarding service.

### *Contact Information*

#### **Domestic (United States)**

---

1. Call **1-888-786-7999**
2. Select *option 3*

#### **International**

---

1. Call **+1-714-282-6111**
2. Select *option 3*

#### **E-Mail**

---

For non-emergency assistance, email us at [\*\*support@m86security.com\*\*](mailto:support@m86security.com)

## **Office Locations and Phone Numbers**

---

### **M86 Corporate Headquarters (USA)**

828 West Taft Avenue  
Orange, CA 92865-4232  
USA

Local : 714.282.6111  
Fax : 714.282.6116  
Domestic US : 1.888.786.7999  
International : +1.714.282.6111

### **M86 Taiwan**

7 Fl., No. 1, Sec. 2, Ren-Ai Rd.  
Taipei 10055  
Taiwan, R.O.C.

Taipei Local : 2397-0300  
Fax : 2397-0306  
Domestic Taiwan : 02-2397-0300  
International : 886-2-2397-0300

## ***Support Procedures***

When you contact our technical support department:

- You will be greeted by a technical professional who will request the details of the problem and attempt to resolve the issue directly.
- If your issue needs to be escalated, you will be given a ticket number for reference, and a senior-level technician will contact you to resolve the issue.
- If your issue requires immediate attention, such as your network traffic being affected or all blocked sites being passed, you will be contacted by a senior-level technician within one hour.
- Your trouble ticket will not be closed until your permission is confirmed.

# Product Warranties

## *Standard Warranty*

M86 Security warrants the medium on which the M86 product is provided to be free from defects in material and workmanship under normal use for period of one year (the “Warranty Period”) from the date of delivery. This standard Warranty Period applies to both new and refurbished equipment for a period of one year from the delivery date. M86 Security’s entire liability and customer’s exclusive remedy if the medium is defective shall be the replacement of the hardware equipment or software provided by M86 Security.

M86 Security warrants that the M86 product(s) do(es) not infringe on any third party copyrights or patents. This warranty shall not apply to the extent that infringement is based on any misuse or modification of the hardware equipment or software provided. This warranty does not apply if the infringement is based in whole or in part on the customer’s modification of the hardware equipment or software.

M86 Security specifically disclaims all express warranties except those made herein and all implied warranties; including without limitation, the implied warranties of merchantability and fitness for a particular purpose. Without limitation, M86 Security specifically disclaims any warranty related to the performance(s) of the M86 product(s). Warranty service will be performed during M86 Security’s regular business hours at M86 Security’s facility.



## ***Technical Support and Service***

M86 Security will provide initial installation support and technical support for up to 90 days following installation. M86 Security provides after-hour emergency support to M86 server customers. An after hours technician can be reached by voice line.

Technical support information:

Online: <http://www.m86security.com/support/>

Toll Free: 888-786-7999, *press 3*

Telephone: 1+714-282-6111, *press 3*

E-mail: [support@m86security.com](mailto:support@m86security.com)

Have the following information ready before calling technical support:

Product Description: \_\_\_\_\_

Purchase Date: \_\_\_\_\_

Extended warranty purchased: \_\_\_\_\_

Plan # \_\_\_\_\_

Reseller or Distributor contact: \_\_\_\_\_

Customer contact: \_\_\_\_\_

## ***Extended Warranty (optional)***

The extended warranty applies to hardware and software of the product(s) except any misuse or modification of the product(s), or product(s) located outside of the United States. The extended warranty does not include new product upgrades. Hardware parts will be furnished as necessary to maintain the proper operational condition of the product(s). If parts are discontinued from production during the Warranty Period, immediate replacement product(s) or hardware parts will be available for exchange with defective parts from M86 Security's local reseller or distributor.

## ***Extended Technical Support and Service***

Extended technical support is available to customers under a Technical Support Agreement. Contact M86 Security during normal business hours, 8 a.m. to 5 p.m. PST, at (888) 786-7999, or if outside the United States, call 1+(714) 282-6111.

# APPENDICES SECTION

## Appendix A

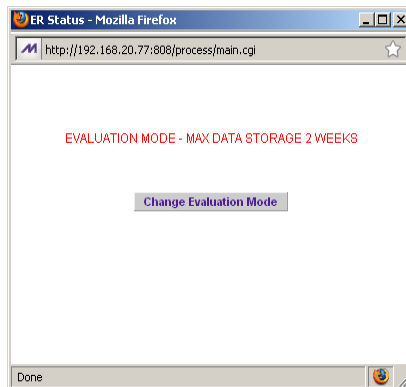
### *Evaluation Mode*

By default, the ER Server and Client are set to the evaluation mode. This appendix explains how to use the ER Server in the evaluation mode, and how to activate the ER Server to function in the activated mode.

### Administrator Console

---

When accessing the **Server > Server Status** screen for the first time, the ER Status pop-up box opens to inform you that the ER unit is currently in the evaluation mode:



*Fig. A-1 ER Status pop-up box*

The Server will store data for the period specified in the pop-up box: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS”—in which ‘X’ represents the maximum number of weeks in the ER’s data storage scope.

You have the option to either use the ER unit in the evaluation mode, or change the evaluation mode in one of two ways—by extending the evaluation period, or by activating the unit so that it can be used in the activated mode.



**NOTE:** *The message: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS” also displays at the top of the Expiration screen in the Administrator console. Refer to the Expiration screen sub-section in Chapter 2 of the Administrator Section for more information about data storage and expiration.*

## Use the Server in the Evaluation Mode

To use the unit in the evaluation mode, click the "X" in the upper right corner of the ER Status pop-up box to close it.

### Expiration screen

In the evaluation mode, the Expiration screen can only be used for viewing data storage statistics, and not for modifying data storage capacity criteria.

The screenshot shows the 'Expiration' screen in Enterprise Reporter M86 Security. The status is as of 2009-12-23 01:27:34. A red banner indicates 'EVALUATION MODE - MAX DATA STORAGE 2 WEEKS'. Below this, a link is provided to activate the box. The main content area lists various statistics:

Date scope for total data	2009-12-11 00:09:26 - 2009-12-23 00:09:44
Total number of week(s) stored	2 week(s)
Current live data (yearweekno/date scope)	200949 - 200951 2009-12-11 00:09:26 - 2009-12-23 00:09:44
Total number of live week(s)	2 week(s)
Current archive data (yearweekno/date scope)	0 - 0 0 - 0
Total number of archive week(s)	0 week(s)
Database disk space utilization (used database space/total database space)	3.44 % (1.73/50.33 Gbytes)
Target percentage of live data	100 %
Last 8 weeks hits/day average	112849
Estimated total week(s) of live data	226 week(s)
Estimated total week(s) of archive data	0 week(s)
Estimated number of week(s) until next expiration	49 week(s)

Below the statistics is a 'Change Settings' section with the following fields:

Hits/day	112849
Percentage of live data	100 %
<input type="button" value="Calculate"/>	
Estimated total week(s) of live data	<input type="text"/> week(s)
Estimated total week(s) of archive data	<input type="text"/> week(s)

Fig. A-2 Expiration screen

When the Server is in the evaluation mode, the following message displays at the top of the screen: “Evaluation Mode – Max Data Storage ‘X’ Weeks” (in which ‘X’ represents the maximum number of weeks in the ER’s data storage scope).

Since the evaluation period is set for a fixed time period, you cannot make adjustments to the amount of data that will be stored on the Server. Thus, the **Save** button is not included at the bottom of the screen.

## Change the Evaluation Mode

After the designated evaluation period has expired, you may extend your evaluation period, or activate the unit and use it in the activated mode. There are two ways to change the evaluation mode from the Administrator console:

- in the ER Status pop-up box (see Fig. A-1), click **Change Evaluation Mode**
- in the Evaluation screen, click the link (“here”) in the message at the top of the screen: “Please click [here](#) to activate the box”.

By clicking the button or link, the Activation Page pop-up box opens:

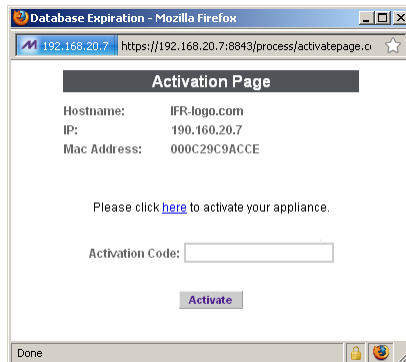


Fig. A-3 Activation Page pop-up box

## **Activation Page**

1. In the Activation Page pop-up box, the **Hostname** of the Server, **IP** address, and **Mac Address** (Media Access Control address) display.
2. In the message “Please click [here](#) to activate your appliance.”, click the link ‘[here](#)’ to open the Product Activation page at the M86 Security Web site.
3. In this Web page:
  - a. Enter your following information: Contact Details, Company Information, and Enterprise Reporter Information.
  - b. Choose the Activation Type: "Evaluation Extension" or "Full Activation."
4. Click **Send Information**. After M86 obtains your information, a technical support representative will issue you an activation code.
5. Return to the Activation Page (see Fig. A-3) and enter the activation code in the **Activation Code** field.
6. Click **Activate** to display the confirmation message in the Activation Page pop-up box:
  - If extending the evaluation period for the unit, the following message displays: “It is now in evaluation mode (‘X’ weeks)!” in which ‘X’ represents the number of weeks in the new evaluation period.
  - If activating the unit, the following message displays: “Your box has been activated!”
7. Click the ‘X’ in the upper right corner to close the Activation Page pop-up box.

# Appendix B

## ***Disable Pop-up Blocking Software***

A user with pop-up blocking software installed on his/her workstation will need to disable pop-up blocking in order to use the Client.

This appendix provides instructions on how to disable pop-up blocking software for the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, and Windows XP Service Pack 2 (SP2).

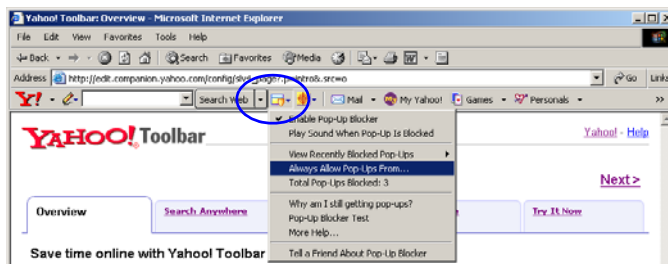
## ***Yahoo! Toolbar Pop-up Blocker***

### **Add the Client to the White List**

---

If the Client was previously blocked by the Yahoo! Toolbar, it can be moved from the black list and added to the white list so that it will always be allowed to pass. To do this:

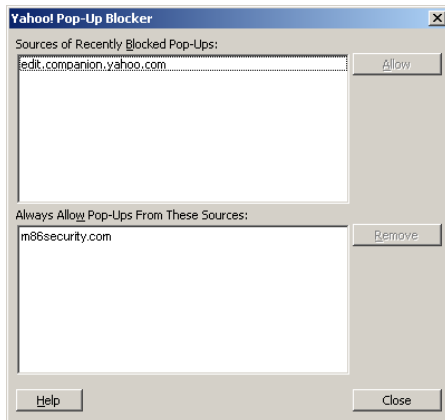
1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:



*Fig. B-1 Select menu option Always Allow Pop-Ups From*



2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:



*Fig. B-2 Allow pop-ups from source*

3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.
4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.
5. Click **Close** to save your changes and to close the dialog box.

## Google Toolbar Pop-up Blocker

### Add the Client to the White List

To add the Client to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the # blocked icon:

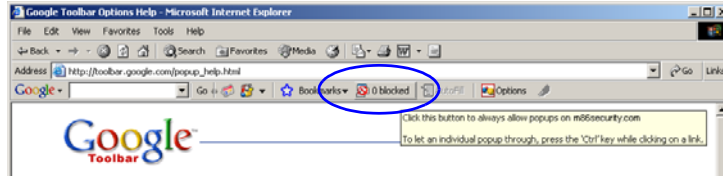


Fig. B-3 # blocked icon enabled

Clicking this icon toggles to the Site pop-ups allowed icon, adding the Client to your white list:

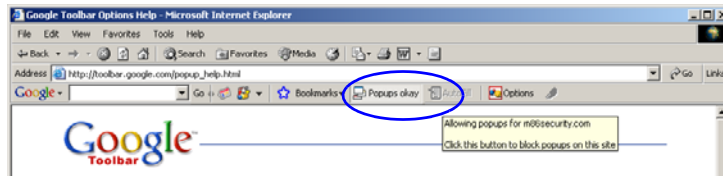


Fig. B-4 Site pop-ups allowed icon enabled

## ***AdwareSafe Pop-up Blocker***

### **Disable Pop-up Blocking**

---

AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.
2. After you are finished using the Client, go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # popups blocked. This action turns on pop-up blocking again.

## Windows XP SP2 Pop-up Blocker

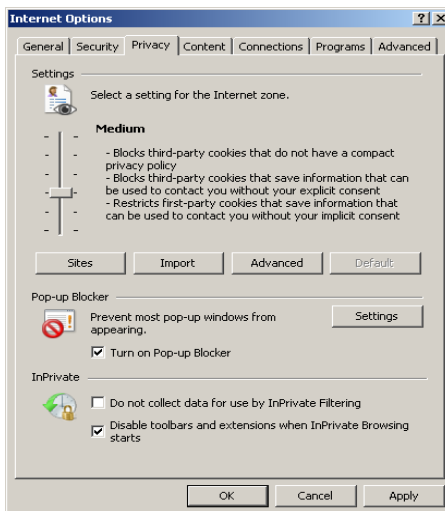
This sub-section provides information on setting up pop-up blocking and disabling pop-up blocking in Windows XP SP2.

### Set up Pop-up Blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

#### Use the Internet Options dialog box

1. From the IE browser, go to the toolbar and select **Tools > Internet Options** to open the Internet Options dialog box.
2. Click the Privacy tab:

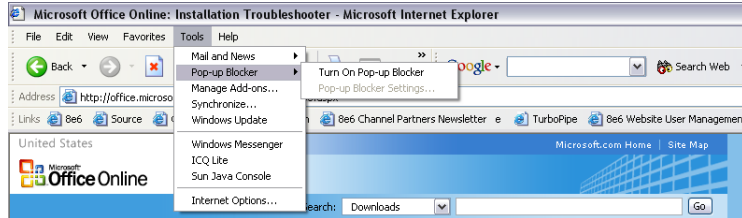


*Fig. B-5 Enable pop-up blocking*

3. In the Pop-up Blocker frame, check “Block pop-ups”.
4. Click **Apply** and then click **OK** to close the dialog box.

## Use the IE Toolbar

In the IE browser, go to the toolbar and select **Tools > Pop-up Blocker > Turn On Pop-up Blocker**:



*Fig. B-6 Toolbar setup*

When you click Turn On Pop-up Blocker, this menu selection changes to Turn Off Pop-up Blocker and activates the Pop-up Blocker Settings menu item.

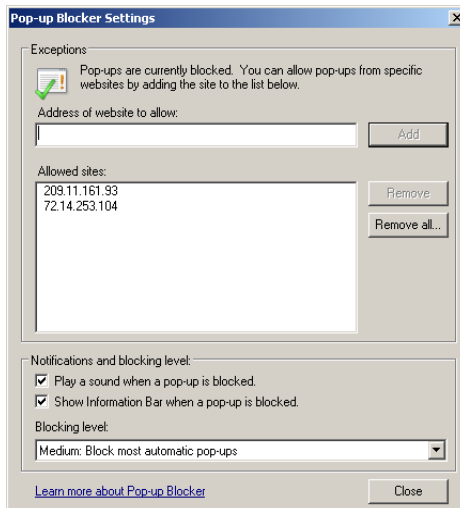
You can toggle between the On and Off settings to enable or disable pop-up blocking.

## Add the Client to the White List

There are two ways to disable pop-up blocking for the Client and to add the Client to your white list.

### Use the IE Toolbar

1. With pop-up blocking enabled, go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box:



*Fig. B-7 Pop-up Blocker Settings*

2. Enter the **Address of Web site to allow**, and click **Add** to include this address in the Allowed sites list box. Click **Close** to close the dialog box. The Client has now been added to your white list.

## Use the Information Bar

With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

### Set up the Information Bar

1. Go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box (see Fig. B-7).
2. In the Notifications and Filter Level frame, click the checkbox for “Show Information Bar when a pop-up is blocked.”
3. Click **Close** to close the dialog box.

### Access the Client

1. Click the Information Bar for settings options:

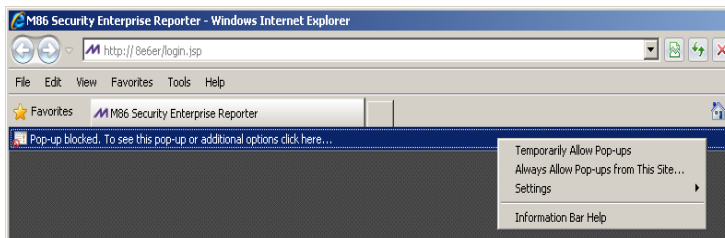


Fig. B-8 Information Bar menu options

2. Select **Always Allow Pop-ups from This Site**—this action opens the Allow pop-ups from this site? dialog box:

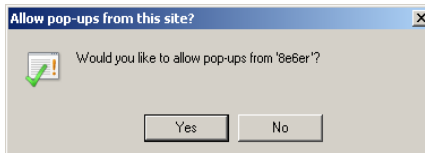


Fig. B-9 Allow pop-ups dialog box

3. Click **Yes** to add the Client to your white list and to close the dialog box.



**NOTE:** *To view your white list, go to the Pop-up Blocker Settings dialog box (see Fig. B-7) and see the entries in the Allowed sites list box.*



# Appendix C

## ***RAID Maintenance and Troubleshooting***

This appendix pertains to ER “H”, “SL”, and “HL” servers and is divided into three parts: Hardware Components, Server Interface, and Troubleshooting—in the event of a failure in one of the drives, power supplies, or fans.



**NOTE:** *As part of the ongoing maintenance procedure for your RAID server, M86 Security recommends that you always have a spare drive and spare power supply on hand.*

Contact M86 Security Technical Support for replacement hard drives and power supplies.

### **Part 1: Hardware Components**

---

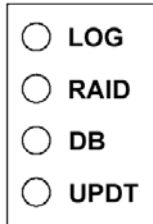
The ER “H”, “SL”, and “HL” RAID server contains four hard drives, two power supplies, and five sets of dual cooling fans (10 in total).

## Part 2: Server Interface

---

### LED indicators in SL and HL units

On an “SL” and “HL” unit, the following LED indicators for software and hardware status monitoring display on the left side of the front panel:



- LOG = Log Download Status
- RAID = Hard Drive Status
- DB = Database Status
- UPDT = Software Update Status

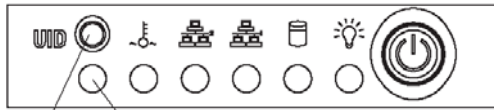
**LED Indicator Chart**

Below is a chart of LED indicators in the “SL” and “HL” unit:

<b>LED Indicator</b>	<b>Color</b>	<b>Condition</b>	<b>Description</b>
LOG	Green	On	Downloading a log
	--	Off	No log download detected
RAID	Green	On	RAID mode enabled and running
	--	Off	RAID mode is inactive
	Red	On	Check user interface for status of hard drive
DB	Green	On	Database is active
	Red	On	Database in inactive
UPDT	Amber	On	Software update detected
	--	Off	No software update detected

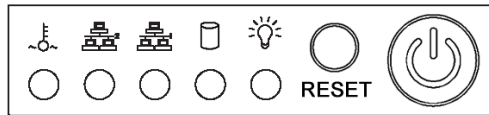
## Front control panels on H, SL, and HL units

Control panel buttons, icons, and LED indicators display on the right side of the front panel. The buttons let you perform a function on the unit, while an LED indicator corresponding to an icon alerts you to the status of that feature on the unit.



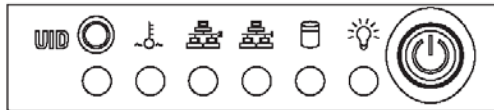
Button LED

*“H” chassis front panel*



OH  
NIC2  
NIC1  
HD  
PWR

*“SL” chassis front panel*



UID  
OH  
NIC2  
NIC1  
HD  
PWR

*“HL” chassis front panel*

The buttons and LED indicators for the depicted icons function as follows:



**UID** (button) – On an “H” or “HL” server, when the UID button is pressed, a steady blue LED displays on both the front and rear of the chassis (see also Rear of chassis). These indicators are used for easy location of the chassis in a large stack configuration. The LED remains on until the button is pressed a second time.



**Overheat/Fan Fail** (icon) – This LED is unlit unless the chassis is overheated. A flashing red LED indicates a fan failure. A steady red LED (on and not flashing) indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm.



**NIC2** (icon) – A flashing green LED indicates network activity on LAN2. The LED is a steady green with link connectivity, and unlit if there with no link connectivity.



**NIC1** (icon) – A flashing green LED indicates network activity on LAN1. The LED is a steady green with link connectivity, and unlit if there with no link connectivity.



**HDD** (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. Hard drive activity is indicated by a green LED on an “H” or “HL” server, and by an amber LED on an “SL” server. An unlit LED on a drive carrier may indicate a hard drive failure. (See Hard drive failure in the Troubleshooting sub-section for information on detecting a hard drive failure and resolving this problem.)



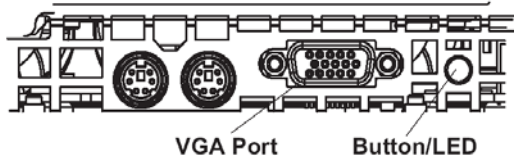
**Power** (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit’s power supplies. (See also Rear of chassis.) (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)



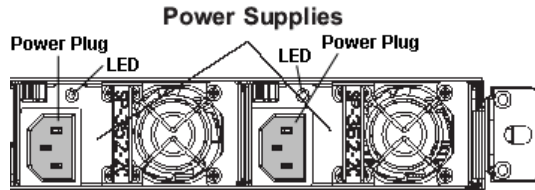
**Power** (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

## Rear panels on H and HL units

**UID (LED indicator)** – On the rear of the “H” or “HL” chassis, to the left of the power supplies, a steady blue UID LED indicator displays when the UID button on the control panel is pressed. This LED remains lit until the UID button is pressed again.



**Power Supplies (LED indicators)** – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs. (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)



---

## Part 3: Troubleshooting

---

The text in this section explains how the server alerts the administrator to a failed component, and what to do in the event of a failure.

### Hard drive failure

#### ***Step 1: Review the notification email***

If a hard drive fails, a notification email is sent to the administrator of the server. This email identifies the failed hard drive by its number (HD 1, HD 2, HD 3, or HD 4). Upon receiving this alert, the administrator should verify the status of the drives by first going to the Hardware Failure Detection screen in the Administrator console.



***WARNING:*** Do not attempt to remove any of the drives from the unit at this time. Verification of the failed drive should first be made in the Administrator console before proceeding, as data on the server will be lost in the event that the wrong drive is removed from the unit.

## Step 2: Verify the failed drive in the Admin console

The Hardware Failure Detection screen in the Administrator console is accessible via the **Server > Hardware Failure Detection** menu selection:

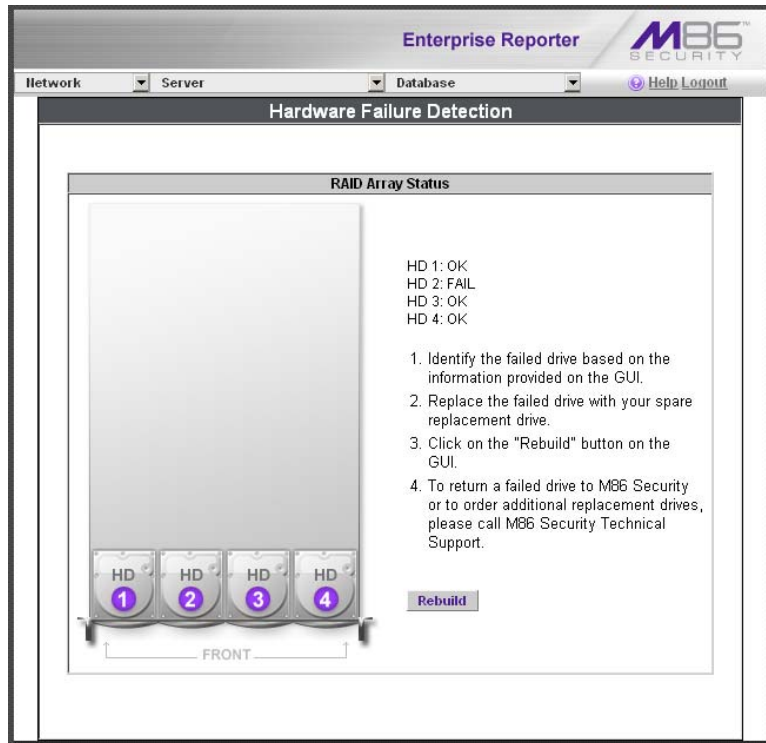


Fig. C-2 Hardware Failure Detection screen

The Hardware Failure Detection screen displays the current RAID Array Status for the four hard drives (HD 1, HD 2, HD 3, and HD 4) in text that appears at the right of the screen.

Normally, when all four hard drives are functioning without failure, the text "OK" displays for the corresponding hard drive number, and no other text displays in the screen.

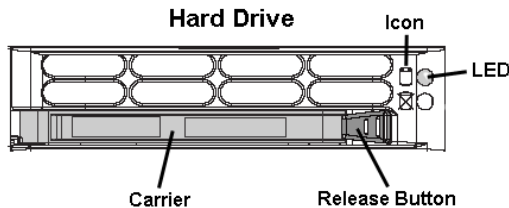
However, if a hard drive has failed, the message "FAIL" displays for the corresponding hard drive number.



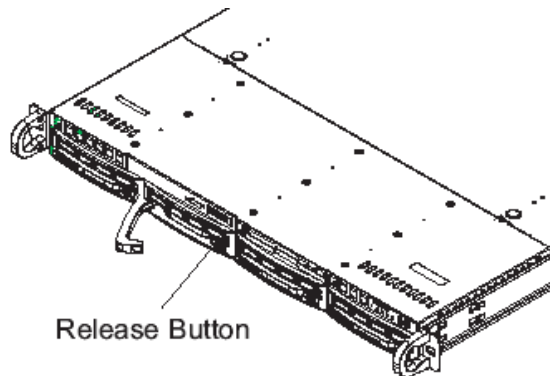
Before taking any action in this screen, proceed to Step 3.


### **Step 3: Replace the failed hard drive**

After verifying the failed hard drive in the Administrator console, go to the server to replace the drive.



Press the red release button to release the handle on the carrier, and then extend the handle fully and pull the carrier out towards you. Replace the failed drive with your spare replacement drive.



 **NOTE:** Contact Technical Support if you have any questions about replacing a failed hard drive.

### **Step 4: Rebuild the hard drive**

Once the failed hard drive has been replaced, return to the Hardware Failure Detection screen in the Administrator console, and click **Rebuild** to proceed with the rebuild process.



**WARNING:** When the RAID array reconstruction process begins, the message “Enterprise Reporter Functionality Suspended, Drive Rebuild in Process” displays and the hard drive becomes inaccessible.

### **Step 5: Contact Technical Support**

Contact Technical Support to order a new replacement hard drive and for instructions on returning your failed hard drive to M86 Security.

## **Power supply failure**

### **Step 1: Identify the failed power supply**

The administrator of the server is alerted to a power supply failure on the chassis by an audible alarm and an amber power supply LED—or an unlit LED—on the front and rear of the chassis.



**NOTE:** A steady amber power supply LED also may indicate a disconnected or loose power supply cord. Verify that the power supply cord is plugged in completely before removing a power supply.



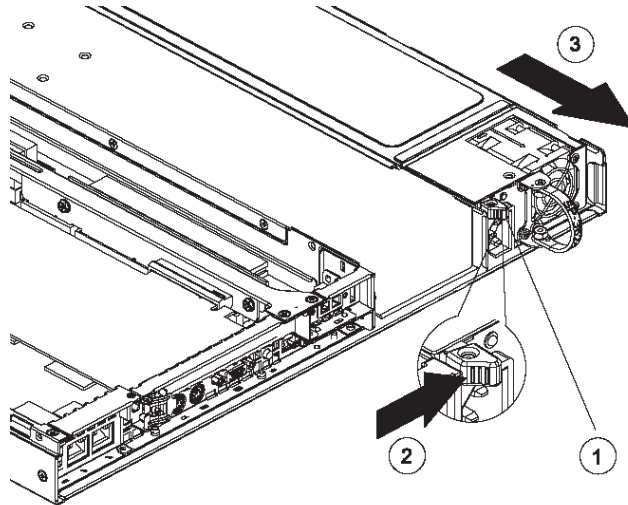
**WARNING:** Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.

### **Step 2: Unplug the power cord**

To prevent electrical shock to yourself and damage to the unit, unplug the power cord from the failed power supply.

### **Step 3: Replace the failed power supply**

Remove the failed power supply by locating the red release tab (1) and pushing it to the right (2), then lifting the curved metal handle and pulling the power supply module towards you (3).



Note that an audible alarm sounds and the LED is unlit when the power supply is disengaged. Replace the failed power supply with your spare replacement power supply. The alarm will turn off and the LED will be a steady green when the replacement power supply is securely locked in place.

### **Step 4: Contact Technical Support**

Contact Technical Support to order a new replacement power supply and for instructions on returning your failed power supply to M86 Security.

## Fan failure

### *Identify a fan failure*

A flashing red LED indicates a fan failure. If this displays on your unit, contact Technical Support for an RMA (Return Merchandise Authorization) number and for instructions on returning the unit to M86 Security.

A steady red LED (on and not flashing) indicates an over-heating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the over-heating condition exists.

---

# INDEX

## A

- Access Client 62
- add/edit/delete administrators 13
- Add/Edit/Delete Administrators screen 18
- administrator
  - e-mail contact setup 43
  - log in to Server 13
- Administrator console 15
- alert box, terminology 4
- archive
  - data setup on Server 84
  - terminology 85

## B

- back up data
  - internal on demand backup 40
  - to remote server 41
- backup
  - procedures 38
- Backup screen 38
- Block Request Count 94
- Blocked Searched Keywords 94
- Box Mode screen 16
- button, terminology 4

## C

- checkbox, terminology 4
- components 8
- consolidated ER 12, 37, 65, 68, 85, 92
- Consolidated Mode 11
- Consolidated Mode Setting screen 65
- Conventions 3

## D

- data storage setup 84

- Database Menu 68
- database status logs 80
- Date Scope
  - Expiration screen 84
- diagnostic reports 80
- Diagnostics 30
- dialog box, terminology 4
- disable pop-up blockers 112

## E

- Elapsed Time 76
- ER Client 7, 15, 16, 18, 27, 68, 91
  - diagnostic reports 81
  - evaluation mode 107
  - troubleshoot problems 80
- expiration 86
- Expiration screen 84
- expire
  - data from Server 84
  - passwords 96
  - terminology 86

## F

- field, terminology 5
- File Transfer Protocol (FTP) 40, 59
- Firefox 9
- frame, terminology 5
- FTP (File Transfer Protocol) 40, 41, 42, 59

## G

- generate
  - static table of IP addresses, machine names 71

## H

- hardware 8
- Hardware Failure Detection screen 63
- HL server 121
- HTTPS 7, 9

login *10*

## I

install

    software update *54*

Installation Guide *7, 10*

Internet Explorer *9, 115*

IP.ID *68*

## L

LDAP *99*

LED indicators *122*

Linux OS *8*

list box, terminology *5*

live

    data setup on Server *84*

    terminology *85*

Locked-out Accounts and IPs screen *21*

lockout *97*

log

    database status *81*

    off the Server *14*

    on the Server *11*

## M

Macintosh *9*

Manual Backup button *40*

Manual Restore button *42*

MySQL *1, 8, 60*

## N

Network Diagnostics screen *30*

Network Menu *15*

network requirements *9*

Network Settings screen *23*

Network Time Protocol (NTP) *28*

NTP (Network Time Protocol) *28*

**O**

- Object Count 95
- Optional Features screen 92

**P**

- Page Count 95
- Page Definition screen 78
- Page View Elapsed Time screen 76
- password
  - create for Administrator GUI 13
  - create for remote server's FTP account 40
  - security option 96
- Ping 31
- pop-up blocking, disable 112
- pop-up box/window, terminology 5
- Product Warranties section 104
- Proxy Setting 58
- pull-down menu, terminology 5

**R**

- radio button, terminology 6
- RAID 63, 121
- Regional Setting screen 27
- remote server backup 41
- reports
  - diagnostic 81
- restart the Server 59
- restore data from backup 42
- rollup 66
- Routing Table screen 25
- rules
  - elapsed time 77
  - expiration 86

**S**

- Safari 9
- screen, terminology 6
- Search String Reporting 94



Secure Access screen 49  
Self Monitoring screen 43  
Server  
    add, maintain routers 25  
    download software update 52  
    perform manual backup 40  
    restart 59  
    restore data from previous backup 42  
    set time 27  
    set up IP addresses 23  
    shut down 59  
    store data, change settings 84  
Server Menu 37  
Server Status screen 47  
Shut Down screen 59  
SL server 121  
SMTP Server Setting screen 45  
SNMP screen 34  
software 8  
    unapply 53  
Software Update screen 52  
Software Update Setting screen 57  
SSL Certificate screen 36  
system requirements 9

## T

table, terminology 6  
technical support 49, 101  
Terminology 4  
text box, terminology 6  
Tools screen 80  
Trace Route 32

## U

update  
    NTP server settings 28  
    routing table 26  
    software 52  
User Group Import screen 99

User Name Identification screen 68  
Username Display Setting screen 73

## **V**

view  
    diagnostic reports 81

## **W**

Wall Clock Time 95  
Web Client Server Management screen 61  
Web Filter 37, 57, 99  
window, terminology 6  
workstation requirements 9